CSD496	**MINI PROJECT**	**CATEGORY**	**L**	**T**	**P**	**CREDIT**	**YEAR OF INTRODUCTION**
		PWS	**0**	**0**	**3**	**2**	**2019**

Preamble: The objective of this course is to apply the fundamental concepts of courses learned in respective Honors Streams: Security in Computing, Machine Learning and Formal Methods. This course helps the learners to get an exposure to the development of application software/hardware solutions/ software simulations in the field of Computer Science and Engineering. It enables the learners to understand the different steps to be followed such as literature review and problem identification, preparation of requirement specification &design document, testing, development and deployment. Mini project enables the students to boost their skills, widen the horizon of thinking and their ability to resolve real life problems.

Prerequisite: A sound knowledge in courses studied in respective honor stream.

Course Outcomes: After the completion of the course the student will be able to

CO#	CO
CO1	Identify technically and economically feasible problems **(Cognitive Knowledge Level: Apply)**
CO2	Identify and survey the relevant literature for getting exposed to related solutions. **(Cognitive Knowledge Level: Apply)**
CO3	Perform requirement analysis, identify design methodologies and develop adaptable & reusable solutions of minimal complexity by using modern tools & advanced programming techniques (**Cognitive Knowledge Level: Apply)**
CO4	Prepare technical report and deliver presentation **(Cognitive Knowledge Level: Apply)**
CO5	Apply engineering and management principles to achieve the goal of the project **(Cognitive Knowledge Level: Apply)**

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
CO2	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
CO3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CO4	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
CO5	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Lifelong learning

Assessment Pattern

Mark Distribution

Total Marks	CIE Marks	ESE Marks
150	75	75

Continuous Internal Evaluation Pattern:

Attendance **10 marks**

Project Guide **15 marks**

Project Report **10 marks**

Evaluation by the Committee (will be evaluating the level of completion
and demonstration of functionality/specifications, presentation,
oral examination, work knowledge and involvement) : **40 marks**

Student Groups with 4 or 5 members should identify a topic of interest in consultation with a Faculty Advisor/Project Coordinator/Guide. Review the literature and gather information pertaining to the chosen topic. State the objectives and develop a methodology to achieve the objectives. Carryout the design/fabrication or develop codes/programs to achieve the objectives by strictly following steps specified in the teaching plan. Innovative design concepts, performance, scalability, reliability considerations, aesthetics/ergonomic, user experience and security aspects taken care of in the project shall be given due weight.

The progress of the mini project is evaluated based on a minimum of two reviews. The review committee may be constituted by a senior faculty member, Mini Project coordinator and project guide. The internal evaluation shall be made based on the progress/outcome of the project, reports and a viva-voce examination, conducted internally by a 3-member committee. A project report is required at the end of the semester. The project has to be demonstrated for its full design specifications.

End Semester Examination Pattern:

The marks will be distributed as

Presentation	: **30 marks**
Demo	: **20 marks**
Viva	: **25 marks.**
Total	: **75 marks.**

TEACHING PLAN

Students are expected to follow the following steps.

1. Review of Literature and Identification of a problem
2. Create an abstract with a problem statement, solution approach, technology stack, team, etc.
3. Create Requirements Specification
4. Create Design Document . This may include designs like,
    a. System Architecture Design
    b. Application Architecture Design
    c. GUI Design
    d. API Design
    e. Database Design
    f. Technology Stack
5. Deployment, Test Run & Get Results
6. Prepare Project Report

Guidelines for the Report preparation

A bonafide report on the mini project shall be submitted within one week after the final presentation. Minimum number of pages should be 40.

- Use Times New Roman font for the entire report – Chapter/Section Title – Times New Roman18, Bold; Heading 2 – Times New Roman16, Bold; Heading 3 – Times New Roman14, Bold; Body- Times New Roman 12, Normal.
- Line Spacing – Between Heading 2 – 3 lines, between lines in paragraph 1.5 lines.

- Alignments – Chapter/Section Title – Center, Heading 2 & 3 should be Left Aligned. Ensure that all body text is paragraph justified.
- Figures & Tables – Ensure that all Figures and Tables are suitably numbered and given proper names/headings. Write figuretitle under the figure and table title above the table.

- **Suggestive order of documentation:**
  i. Top Cover
  ii. Title page
  iii. Certification page
  iv. Acknowledgment
  v. Abstract
  vi. Table of Contents
  vii. List of Figures and Tables
  viii. Chapters
  ix. Appendices, if any
  x. References/Bibliography

CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT	Year of Introduction
CST 292	**Number Theory**	**Honours**	**4**	**0**	**0**	**4**	**2019**

Preamble: This is the foundational course for awarding B. Tech. Honours in Computer Science and Engineering with specialization in ***Security in Computing***. The purpose of this course is to create awareness among learners about the important areas of number theory used in computer science. This course covers Divisibility & Modular Arithmetic, Primes & Congruences, Euler's Function, Quadratic Residues and Arithmetic Functions, Sum of Squares and Continued fractions. Concepts in Number Theory help the learner to apply them eventually in practical applications in Computer organization & Security, Coding & Cryptography, Random number generation, Hash functions and Graphics.

Prerequisite: A sound background in Higher Secondary School Mathematics

Course Outcomes: After the completion of the course the student will be able to

CO1	Illustrate modular arithmetic operations, methods and techniques **(Cognitive Knowledge Level:Understand)**
CO2	Use the methods - Induction, Contraposition or Contradiction to verify the correctness of mathematical assertions **(Cognitive Knowledge Level: Apply)**
CO3	Utilize theorems and results about prime numbers, congruences, quadratic residues and integer factorization for ensuring security in computing systems **(Cognitive Knowledge Level: Analyse)**
CO4	Illustrate uses of Chinese Remainder Theorem & Euclidean algorithm in Cryptography and Security **(Cognitive Knowledge Level: Apply)**
CO5	Explain applications of arithmetic functions in Computer Science **(Cognitive Knowledge Level:Understand)**
CO6	Implement Number Theoretic Algorithms using a programming language **(Cognitive Knowledge Level: Apply)**

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✓	✓	✓	✓						✓		✓
CO2	✓	✓	✓	✓								✓
CO3	✓	✓	✓	✓		✓						✓
CO4	✓	✓	✓	✓		✓						✓
CO5	✓	✓	✓	✓						✓		✓
CO6	✓	✓	✓	✓	✓			✓				✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		End Semester Examination Marks (Percentage)
	Test1 (Percentage)	Test2 (Percentage)	
Remember	30	30	30
Understand	30	30	30
Apply	40	40	40
Analyse			
Evaluate			
Create			

Mark Distribution

Total Marks	CIE Marks	ESE Marks	ESE Duration
150	**50**	**100**	**3 hours**

Continuous Internal Evaluation Pattern:

Attendance	**:** 10 marks
Continuous Assessment Tests	**:** 25 marks
Continuous Assessment Assignment	**:** 15 marks

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks

First Internal Examination shall be preferably conducted after completing the first half of the syllabus and the Second Internal Examination shall be preferably conducted after completing remaining part of the syllabus.

There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly covered module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly covered module), each with 7 marks. Out of the 7 questions in Part B, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which a student should answer any one. Each question can have maximum 2 sub-divisions and carries 14 marks.

SYLLABUS

Module 1

Divisibility and Modular Arithmetic:

Finite Fields – Groups, Rings and Fields.

Divisibility - Divisibility and Division Algorithms, Well ordering Principle,Bezout's Identity.

Modular Arithmetic- Properties, Euclid's algorithm for the greatest common divisor, Extended Euclid's Algorithm, Least Common multiple, Solving Linear Diophantine Equations, Modular Division.

Module 2

Primes and Congruences:

Prime Numbers-Prime Numbers andprime-powerfactorization, Fermat and Mersenne primes., Primality testing and factorization.

Congruences-Linear congruences, Simultaneous linear congruences, Chinese Remainder Theorem, Fermat’s little theorem, Wilson's theorem.

Module 3

Congruences with a Prime-Power Modulus&Euler's Function:

Congruences with a Prime-Power Modulus-Arithmetic modulo p, Pseudoprimes and Carmichael numbers, Solving congruences modulo prime powers.

Euler's Function-Euler’s Totient function, Applications of Euler’s Totient function, Traditional Cryptosystem, Limitations.

The Group of units- The group U_n,Primitive roots, Existence of primitive roots, Applications of primitive roots.

Module 4

Quadratic Residues & Arithmetic Functions :

Quadratic Residues- Quadratic Congruences, The group of Quadratic residues, Legendre symbol, Jacobi Symbol, Quadratic reciprocity.

Arithmetic Functions- Definition and examples, Perfect numbers, Mobius function and its properties, Mobius inversion formula, The Dirichlet Products.

Module 5

Sum of Squares and Continued Fractions:

Sum of Squares- Sum of two squares, The Gaussian Integers, Sum of three squares, Sum of four squares.

Continued Fractions -Finite continued fractions, Infinite continued fractions, Pell's Equation, Solution of Pell’s equation by continued fractions.

Text Books

1. G.A. Jones & J.M. Jones, Elementary Number Theory, Springer UTM, 2007.

2. Joseph Silverman, A Friendly introduction to Number Theory, Pearson Ed. 2009.

Reference Books

1. William Stallings, Cryptography and Network Security Principles and Practice, Pearson Ed.
2. Tom M.Apostol, ‘Introduction to Analytic Number Theory’, Narosa Publishing House Pvt. Ltd, New Delhi, (1996).
3. Neal Koblitz, A course in Number Theory and Cryptography, 2nd Edition, Springer ,2004.

Sample Course Level Assessment Questions

Course Outcome 1 (CO1): Describe the properties of modular arithmetic and modulo operator.

Course Outcome 2 (CO2): Prove that the equation $y^2 = x^3 - 2$ has only the integer solution (3, ±5).

Course Outcome 3 (CO3): State the law of reciprocity for Jacobi symbols and use it to determine whether 888 is a quadratic residue or non residue of the prime 1999.

Course Outcome 4 (CO4): Using Chinese remainder theorem, solve the system of congruence $x \equiv 2 (\mathrm{mod}\ 3)$, $x \equiv 3 (\mathrm{mod}\ 5)$, $x \equiv 2 (\mathrm{mod}\ 7)$

Course Outcome 5(CO5): State and prove Dirichlet product.

Course Outcome 6 (CO6): Use extended Euclid's algorithm to solve Diophantine equations efficiently. Given three numbers a>0, *b*>0, and *c*, the algorithm should return some *x* and *y* such that a x + b y = c.

Model Question Paper

QP CODE: PAGES: 03

RegNo : …............................... Name :………..……………

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY
FOURTH SEMESTER BTECH (HONOURS) DEGREE EXAMINATION, MONTH &YEAR

Course Code:CST 292 Course
Name: Number Theory

Max.Marks:100 **Duration: 3 Hours**

PART A

Answer all Questions. Each question carries 3 Marks (10x3=30)

1. State and prove well ordering principle.
2. Find gcd d of x=525 and y=231 and express d as ax + by where a and b are integers.
3. Solve the congruence equation 103 x≡ 57 (mod 211).
4. Use Fermat's Little theorem to show that 91 is not a prime.
5. If m is relatively prime to n , show that $\Phi(mn) = \Phi(m)\ \Phi(n)$.
6. Explain how public key cryptography can be used for digital signatures.
7. Define Mobius function and prove Mobius function is a multiplicative.
8. State and prove Dirichlet product.
9. Show that every prime of the form 4k+1 canbe represented uniquely as the sum of two squares.
10. Find the continued fraction representation of the rational number 55/89.

Part B

Answer any one Question from each module.
Each question carries 14 Marks

11. (a) State the Euclidean algorithm and its extension with an example. (7)

    (b) Find all the solutions of 24x + 34 y = 6. (7)

OR

12. (a) Describe the properties of modular arithmetic and modulo operator. (7)

    (b) Explain Extended Euclidean algorithm. Using the algorithm find the multiplicative inverse of 135 mod 61 (7)

13. (a) State and prove Wilson's theorem . (7)

(b) Explain Fermat's factorization method and use it to factor 809009 (7)

OR

14. (a) Using Chinese remainder theorem, solve the system of congruences, $x \equiv 2 (\text{mod } 3)$, $x \equiv 3 (\text{mod } 5)$, $x \equiv 2 (\text{mod } 7)$ (7)

(b) Define Fermat primes. Show that any two distinct Fermat numbers are Relatively prime. (7)

15. (a) Distinguish between public key and private key encryption techniques. Also point out the merits and demerits of both. (7)

(b) Define Carmichael number and show that a Carmichael number must be the product of at least three distinct primes. (7)

OR

16. (a)Define a pseudo prime to a base and find all non trivial bases for which 15 is a pseudo prime. (6)

(b) Find an element of

i) order 5 modulo 11 ii) order 4 modulo 13

iii) order 8 modulo 17 iv) order 6 modulo 19 (8)

17. (a) Determine the quadratic residues and non residues modulo 17. Also determine whether 219 is a quadratic residue or non residue of the prime 383. (8)

(b) State the law of quadratic reciprocity. Determine those odd primes p for which 3 is a quadratic residue and those for which it is a non residue. (6)

OR

18. (a) State and prove properties of Legendre's symbol. (7)

(b) State the law of reciprocity for Jacobi symbols and using it determine whether 888 is a quadratic residue or non residue of the prime 1999. (7)

19. (a) Prove that the equation $y^2 = x^3 - 2$ has only the integer solution (3 , ±5). (7)

(b) Define a Gaussian integer. Factorize the Gaussian integer 440 − 55i. (7)

OR

20. (a) If *m*, and *n* can be expressed as sum of four squares, then show that *mn* can also be expressed the sum of four squares. (7)

(b) Find all the solutions of the Diophantine equation $x^2 – 6 y^2 =1$. (7)

Teaching Plan

Module 1: Divisibility and Euclidean Algorithm		**9 hours**
1.1	Finite Fields – Groups and Rings.	1 hour
1.2	Finite Fields – Fields.	1 hour
1.3	Divisibility and Division Algorithms, Well ordering Principle.	1 hour
1.4	Decimal Expansion of a positive Integer, Greatest Common Divisor, Bezout's Theorem.	1 hour
1.5	Modular Arithmetic- Properties of congruences, Modular Arithmetic Operations, Properties of Modular Arithmetic.	1 hour
1.6	Euclid's algorithm for the greatest common divisor, Extended Euclid's Algorithm.	1 hour
1.7	Solving Linear Diophantine Equations.	1 hour
1.8	Least Common multiple and Modular Division.	1 hour
1.9	Implementation of Euclid's algorithm, Extended Euclid's Algorithm and solution of Linear Diophantine Equations.	1 hour
Module 2: Primes and Congruences		**9 hours**
2.1	Prime Numbersand prime-powerFactorization.	1 hour
2.2	Fermat and Mersenne primes.	1 hour
2.3	Primality testing and factorization, Miller -Rabin Test for Primality.	1 hour
2.4	Pollard's Rho Method for Factorization, Fermat's Factorization.	1 hour

2.5	Linear congruences, Simultaneous linear congruences.	1 hour
2.6	Chinese Remainder Theorem.	1 hour
2.7	Implementation of Chinese Remainder Theorem.	1 hour
2.8	Fermat's little theorem.	1 hour
2.9	Wilson's theorem.	1 hour
Module 3: Congruences with a Prime-Power Modulus &Euler's Function		**9 hours**
3.1	Congruences with a Prime-Power Modulus, Arithmetic modulo p.	1 hour
3.2	Pseudo-primes and Carmichael numbers.	1 hour
3.3	Solving congruences modulo prime powers.	1 hour
3.4	Definition of Euler Totient function, Examples and properties.	1 hour
3.5	Multiplicativity of Euler's Totient function.	1 hour
3.6	Applications of Euler’s function, Euler’s Theorem.	1 hour
3.7	Traditional Cryptosystem, Limitations, Public Key Cryptography.	1 hour
3.8	The Group of Units, Primitive Roots.	1 hour
3.9	Existence of primitive roots for Primes, Applications of primitive roots.	1 hour
Module 4: Quadratic Residues and Arithmetic Functions		**9 hours**
4.1	Quadratic congruences, The group of Quadratic Residues.	1 hour
4.2	Legendre symbol, Jacobi Symbol.	1 hour
4.3	Quadratic reciprocity.	1 hour
4.4	Quadratic residues for prime-power moduli.	1 hour
4.5	Arithmetic Functions: Definition and examples.	1 hour

4.6	Perfect numbers, Definition and proposition.	1 hour
4.7	Mobius inversion formula., application of the Mobius inversion formula.	1 hour
4.8	Mobius function and its properties.	1 hour
4.9	The Dirichlet Product, Definition and proof.	1 hour
Module 5: Sum of Squares and Continued Fractions		**9 hours**
5.1	Sum of Squares, Sum of two squares.	1 hour
5.2	The Gaussian Integers.	1 hour
5.3	Sum of three squares.	1 hour
5.4	Sum of four squares.	1 hour
5.5	Continued Fractions, Finite continued fractions.	1 hour
5.6	Continued Fractions, Finite continued fractions.	1 hour
5.7	Infinite continued fractions.	1 hour
5.8	Pell's Equation, Definition.	1 hour
5.9	Solution of Pell's equation by continued fractions.	1 hour

CODE CST 294	Computational Fundamentals for Machine Learning	CATEGORY	L	T	P	CREDIT
		HONOURS	3	1	0	4

Preamble: This is the foundational course for awarding B. Tech. Honours in Computer Science and Engineering with specialization in ***Machine Learning***. The purpose of this course is to introduce mathematical foundations of basic Machine Learning concepts among learners, on which Machine Learning systems are built. This course covers Linear Algebra, Vector Calculus, Probability and Distributions, Optimization and Machine Learning problems. Concepts in this course help the learners to understand the mathematical principles in Machine Learning and aid in the creation of new Machine Learning solutions, understand & debug existing ones, and learn about the inherent assumptions & limitations of the current methodologies.

Prerequisite: A sound background in higher secondary school Mathematics.

Course Outcomes: After the completion of the course the student will be able to

CO 1	Make use of the concepts, rules and results about linear equations, matrix algebra, vector spaces, eigenvalues & eigenvectors and orthogonality & diagonalization to solve computational problems (Cognitive Knowledge Level: **Apply**)
CO 2	Perform calculus operations on functions of several variables and matrices, including partial derivatives and gradients (Cognitive Knowledge Level: **Apply**)
CO 3	Utilize the concepts, rules and results about probability, random variables, additive & multiplicative rules, conditional probability, probability distributions and Bayes' theorem to find solutions of computational problems (Cognitive Knowledge Level: **Apply**)
CO 4	Train Machine Learning Models using unconstrained and constrained optimization methods (Cognitive Knowledge Level: **Apply**)
CO 5	Illustrate how the mathematical objects - linear algebra, probability, and calculus can be used to design machine learning algorithms (Cognitive Knowledge Level: **Understand**)

Mapping of course outcomes with program outcomes

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
CO 1	√	√	√	√								√
CO 2	√	√	√									√
CO 3	√	√	√	√								√
CO 4	√	√	√	√		√						√
CO 5	√	√	√	√	√	√				√		√

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		End Semester Examination
	1	2	
Remember	20%	20%	20%
Understand	40%	40%	40%
Apply	40%	40%	40%
Analyse			
Evaluate			
Create			

Mark Distribution

Total Marks	CIE Marks	ESE Marks	ESE Duration
150	50	100	3 hours

Continuous Internal Evaluation Pattern:

Attendance : 10 marks

Continuous Assessment Tests : 25 marks

Continuous Assessment Assignment : 15 marks

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks

First Internal Examination shall be preferably conducted after completing the first half of the syllabus and the Second Internal Examination shall be preferably conducted after completing remaining part of the syllabus.

There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly covered module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly covered module), each with 7 marks. Out of the 7 questions in Part B, a student should answer any 5.

End Semester Examination Pattern: There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which student should answer anyone. Each question can have maximum 2 sub-divisions and carries 14 marks.

Syllabus

Module 1

LINEAR ALGEBRA : Systems of Linear Equations – Matrices, Solving Systems of Linear Equations. Vector Spaces - Linear Independence, Basis and Rank, Linear Mappings, Norms, - Inner Products - Lengths and Distances - Angles and Orthogonality - Orthonormal Basis - Orthogonal Complement - Orthogonal Projections. Matrix Decompositions - Determinant and Trace, Eigenvalues and Eigenvectors, Cholesky Decomposition, Eigen decomposition and Diagonalization, Singular Value Decomposition, Matrix Approximation.

Module 2

VECTOR CALCULUS : Differentiation of Univariate Functions - Partial Differentiation and Gradients, Gradients of Vector Valued Functions, Gradients of Matrices, Useful Identities for Computing Gradients. Back propagation and Automatic Differentiation - Higher Order Derivatives- Linearization and Multivariate Taylor Series.

Module 3

Probability and Distributions : Construction of a Probability Space - Discrete and Continuous Probabilities, Sum Rule, Product Rule, and Bayes' Theorem. Summary Statistics and Independence – Important Probability distributions - Conjugacy and the Exponential Family - Change of Variables/Inverse Transform.

Module 4

Optimization : Optimization Using Gradient Descent - Gradient Descent With Momentum, Stochastic Gradient Descent. Constrained Optimization and Lagrange Multipliers - Convex Optimization - Linear Programming - Quadratic Programming.

Module 5

CENTRAL MACHINE LEARNING PROBLEMS : Data and Learning Model- Empirical Risk Minimization - Parameter Estimation - Directed Graphical Models.

Linear Regression - Bayesian Linear Regression - Maximum Likelihood as Orthogonal Projection.

Dimensionality Reduction with Principal Component Analysis - Maximum Variance Perspective, Projection Perspective. Eigenvector Computation and Low Rank Approximations.

Density Estimation with Gaussian Mixture Models - Gaussian Mixture Model, Parameter Learning via Maximum Likelihood, EM Algorithm.

Classification with Support Vector Machines - Separating Hyperplanes, Primal Support Vector Machine, Dual Support Vector Machine, Kernels.

Text book:

1.Mathematics for Machine Learning by Marc Peter Deisenroth, A. Aldo Faisal, and Cheng Soon Ong published by Cambridge University Press (freely available at https:// mml - book.github.io)

Reference books:

1. Linear Algebra and Its Applications, 4th Edition by Gilbert Strang

2. Linear Algebra Done Right by Axler, Sheldon, 2015 published by Springer

3. Introduction to Applied Linear Algebra by Stephen Boyd and Lieven Vandenberghe, 2018 published by Cambridge University Press

4. Convex Optimization by Stephen Boyd and Lieven Vandenberghe, 2004 published by Cambridge University Press

5. Pattern Recognition and Machine Learning by Christopher M Bishop, 2006, published by Springer

6. Learning with Kernels – Support Vector Machines, Regularization, Optimization, and Beyond by Bernhard Scholkopf and Smola, Alexander J Smola, 2002, bublished by MIT Press

7. Information Theory, Inference, and Learning Algorithms by David J. C MacKay, 2003 published by Cambridge University Press

8. Machine Learning: A Probabilistic Perspective by Kevin P Murphy, 2012 published by MIT Press.

9. The Nature of Statistical Learning Theory by Vladimir N Vapnik, 2000, published by Springer

Sample Course Level Assessment Questions.

Course Outcome 1 (CO1):

1. Find the set ***S*** of all solutions in ***x*** of the following inhomogeneous linear systems ***Ax* = *b***, where ***A*** and ***b*** are defined as follows:

$$\boldsymbol{A} = \begin{bmatrix} 1 & -1 & 0 & 0 & 1 \\ 1 & 1 & 0 & -3 & 0 \\ 2 & -1 & 0 & 1 & -1 \\ -1 & 2 & 0 & -2 & -1 \end{bmatrix}, \quad \boldsymbol{b} = \begin{bmatrix} 3 \\ 6 \\ 5 \\ -1 \end{bmatrix}$$

2. Determine the inverses of the following matrix if possible

$$\boldsymbol{A} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

3. Are the following sets of vectors linearly independent?

$$\boldsymbol{x}_1 = \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix}, \quad \boldsymbol{x}_2 = \begin{bmatrix} 1 \\ 1 \\ -2 \end{bmatrix}, \quad \boldsymbol{x}_3 = \begin{bmatrix} 3 \\ -3 \\ 8 \end{bmatrix}$$

4. A set of ***n*** linearly independent vectors in ***R***^{n} forms a basis. Does the set of vectors **(2, 4,−3)** , **(0, 1, 1)** , **(0, 1,−1)** form a basis for ***R***^{3}? Explain your reasons.

5. Consider the transformation ***T (x, y) = (x + y, x + 2y, 2x + 3y)***. Obtain ***ker T*** and use this to calculate the nullity. Also find the transformation matrix for ***T***.

6. Find the characteristic equation, eigenvalues, and eigenspaces corresponding to each eigenvalue of the following matrix

$$\begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \\ 0 & 1 & 2 \end{bmatrix}$$

7. Diagonalize the following matrix, if possible

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

8. Find the singular value decomposition (SVD) of the following matrix

$$\begin{bmatrix} 0 & 1 & 1 \\ \sqrt{2} & 2 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Course Outcome 2 (CO2):

1. For a scalar function ***f(x, y, z)*** $= x^2 + 3y^2 + 2z^2$, find the gradient and its magnitude at the point **(1, 2, -1)**.
2. Find the maximum and minimum values of the function f***(x, y)*** $= 4x + 4y - x^2 - y^2$ subject to the condition $x^2 + y^2 <= 2$.
3. Suppose you were trying to minimize ***f(x, y)*** $= x^2 + 2y + 2y^2$. Along what vector should you travel from (5, 12)?
4. Find the second order Taylor series expansion for ***f(x, y)*** $= (x + y)^2$ about **(0 , 0)**.
5. Find the critical points of ***f(x, y)*** $= x^2 - 3xy + 5x - 2y + 6y^2 + 8$.
6. Compute the gradient of the Rectified Linear Unit (ReLU) function ***ReLU(z)*** = ***max(0 , z)***.
7. Let $L = ||Ax - b||^2_2$, where ***A*** is a matrix and ***x*** and ***b*** are vectors. Derive ***dL*** in terms of ***dx***.

Course Outcome 3 (CO3):

1. Let J and T be independent events, where $P(J)=0.4$ and $P(T)=0.7$.

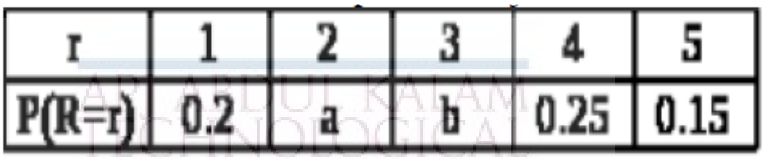
   i. Find $P(J\cap T)$

   ii. Find $P(J\cup T)$

   iii. Find $P(J\cap T')$

2. Let A and B be events such that $P(A)=0.45$, $P(B)=0.35$ and $P(A\cup B)=0.5$. Find $P(A|B)$.

3. A random variable **R** has the probability distribution as shown in the following table:



r	1	2	3	4	5
P(R=r)	0.2	a	b	0.25	0.15

   i. Given that $E(R)=2.85$, find a and b.

   ii. Find $P(R>2)$.

4. A biased coin (with probability of obtaining a head equal to $p > 0$) is tossed repeatedly and independently until the first head is observed. Compute the probability that the first head appears at an even numbered toss.

5. Two players A and B are competing at a trivia quiz game involving a series of questions. On any individual question, the probabilities that A and B give the correct answer are p and q respectively, for all questions, with outcomes for different questions being independent. The game finishes when a player wins by answering a question correctly. Compute the probability that A wins if

   i. A answers the first question,

   ii. B answers the first question.

6. A coin for which $P(heads) = p$ is tossed until two successive tails are obtained. Find the probability that the experiment is completed on the n^{th} toss.

7. You roll a fair dice twice. Let the random variable X be the product of the outcomes of the two rolls. What is the probability mass function of X? What are the expected value and the standard deviation of X?

8. While watching a game of Cricket, you observe someone who is clearly supporting Mumbai Indians. What is the probability that they were actually born within 25KM of Mumbai? Assume that:

    - the probability that a randomly selected person is born within 25KM of Mumbai is 1/20;
    - the chance that a person born within 25KMs of Mumbai actually supports MI is 7/10 ;
    - the probability that a person not born within 25KM of Mumbai supports MI with probability 1/10.

9. What is an exponential family? Why are exponential families useful?
10. Let Z_1 and Z_2 be independent random variables each having the standard normal distribution. Define the random variables X and Y by $X = Z_1 + 3Z_2$ and Y $= Z_1 + Z_2$. Argue that the joint distribution of (X, Y) is a bivariate normal distribution. What are the parameters of this distribution?
11. Given a continuous random variable x, with cumulative distribution function $F_x(x)$, show that the random variable $y = F_x(x)$ is uniformly distributed.
12. Explain Normal distribution, Binomial distribution and Poisson distribution in the exponential family form.

Course Outcome 4(CO4):

1. Find the extrema of $f(x, y) = x$ subject to $g(x, y) = x^2 + 2y^2 = 3$.
2. Maximize the function $f(x, y, z) = xy + yz + xz$ on the unit sphere $g(x, y, z) = x^2 + y^2 + z^2 = 1$.
3. Provide necessary and suffcient conditions under which a quadratic optimization problem be written as a linear least squares problem.
4. Consider the univariate function $f(x) = x^3 + 6x^2 - 3x - 5$. Find its stationary points and indicate whether they are maximum, minimum, or saddle points.
5. Consider the update equation for stochastic gradient descent. Write down the update when we use a mini-batch size of one.

6. Consider the function

$$f(x) = (x_1 - x_2)^2 + \frac{1}{1 + x_1^2 + x_2^2}.$$

   i. Is ***f(x)*** a convex function? Justify your answer.

   ii. Is (1 , -1) a local/global minimum? Justify your answer.

7. Is the function ***f(x, y) = 2x² + y² + 6xy - x + 3y - 7*** convex, concave, or neither? Justify your answer.

8. Consider the following convex optimization problem

$$\text{minimize } \frac{x^2}{2} + x + 4y^2 - 2y$$

   Subject to the constraint ***x + y >= 4, x, y >= 1***.

   Derive an explicit form of the Lagrangian dual problem.

9. Solve the following LP problem with the simplex method.

$$max\ \ 5x_1 + 6x_2 + 9x_3 + 8x_4$$

   subject to the constraints

$$\begin{array}{ccccccccc} x_1 & + & 2x_2 & + & 3x_3 & + & x_4 & \leq & 5 \\ x_1 & + & x_2 & + & 2x_3 & + & 3x_4 & \leq & 3 \end{array}$$

$$x_1, x_2, x_3, x_4 \geq 0$$

Course Outcome 5 (CO5):

1. What is a loss function? Give examples.

2. What are training/validation/test sets? What is cross-validation? Name one or two examples of cross-validation methods.

3. Explain generalization, overfitting, model selection, kernel trick, Bayesian learning

4. Distinguish between Maximum Likelihood Estimation (MLE) and Maximum A Posteriori Estimation (MAP)?

5. What is the link between structural risk minimization and regularization?

6. What is a kernel? What is a dot product? Give examples of kernels that are valid dot products.

7. What is ridge regression? How can one train a ridge regression linear model?

8. What is Principal Component Analysis (PCA)? Which eigen value indicates the direction of largest variance? In what sense is the representation obtained from a projection onto the eigen directions corresponding the the largest eigen values optimal for data reconstruction?

9. Suppose that you have a linear support vector machine (SVM) binary classifier. Consider a point that is currently classified correctly, and is far away from the decision boundary. If you remove the point from the training set, and re-train the classifier, will the decision boundary change or stay the same? Explain your answer in one sentence.

10. Suppose you have ***n*** independent and identically distributed (i.i.d) sample data points $x_1, \ldots , x_n$. These data points come from a distribution where the probability of a given datapoint ***x*** is

$$P(x) = \frac{1}{\theta} e^{-\frac{1}{\theta} x}.$$

    Prove that the MLE estimate of parameter is the sample mean.

11. Suppose the data set $y_1,\ldots,y_n$ is a drawn from a random sample consisting of i.i.d. discrete uniform distributions with range 1 to N. Find the maximum likelihood estimate of ***N***.

12. Ram has two coins: one fair coin and one biased coin which lands heads with probability 3/4. He picks one coin at random (50-50) and flips it repeatedly until he gets a tails. Given that he observes 3 heads before the first tails, find the posterior probability that he picked each coin.

    i. What are the prior and posterior odds for the fair coin?

    ii. What are the prior and posterior predictive probabilities of heads on the next flip? Here prior predictive means prior to considering the data of the first four flips.

Model Question paper

QP Code : **Total Pages: 4**

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

IV SEMESTER B.TECH (HONOURS) DEGREE EXAMINATION, MONTH and YEAR

Course Code: CST 294

Course Name: COMPUTATIONAL FUNDAMENTALS FOR MACHINE LEARNING

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1 Show that with the usual operation of scalar multiplication but with addition on reals given by $x \# y = 2(x + y)$ is not a vector space.

2 Find the eigenvalues of the following matrix in terms of k. Can you find an eigenvector corresponding to each of the eigenvalues?

$$\begin{bmatrix} 1 & k \\ 2 & 1 \end{bmatrix}$$

3 Let $f(x, y, z) = xye^r$, where $r = x^2+z^2-5$. Calculate the gradient of f at the point **(1, 3, -2)**.

4 Compute the Taylor polynomials T_n, $n = 0, \ldots, 5$ of $f(x) = \sin(x) + \cos(x)$ at $x_0 = 0$.

5 Let X be a continuous random variable with probability density function on $0 <= x <= 1$ defined by $f(x) = 3x^2$. Find the pdf of $Y = X^2$.

6 Show that if two events A and B are independent, then A and B' are independent.

7 Explain the principle of the gradient descent algorithm.

8 Briey explain the difference between (batch) gradient descent and stochastic gradient descent. Give an example of when you might prefer one over the other.

9 What is the empirical risk? What is “empirical risk minimization”?

10 Explain the concept of a Kernel function in Support Vector Machines. Why are kernels so useful? What properties a kernel should posses to be used in an SVM?

PART B

Answer any one Question from each module. Each question carries 14 Marks

11 a) i. Find all solutions to the system of linear equations (6)

$$\begin{aligned} -4x + 5z &= -2 \\ -3x - 3y + 5z &= 3 \\ -x + 2y + 2z &= -1 \end{aligned}$$

ii. Prove that all vectors orthogonal to **[2, −3, 1]$^{\mathbf{T}}$** forms a subspace ***W*** of ***R***^{3}. What is ***dim (W)*** and why?

b) Use the Gramm-Schmidt process to find an orthogonal basis for the column space of the following matrix (8)

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

OR

12 a) i. Let $\boldsymbol{L}$ be the line through the origin in $\boldsymbol{R^2}$ that is parallel to the vector **$[3, 4]^T$**. Find the standard matrix of the orthogonal projection onto L. Also find the point on $\boldsymbol{L}$ which is closest to the point **(7 , 1)** and find the point on $\boldsymbol{L}$ which is closest to the point ***(-3 , 5)***. (6)

ii. Find the rank-1 approximation of

$$\begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & -2 \end{bmatrix}$$

b) i. Find an orthonormal basis of $\boldsymbol{R^3}$ consisting of eigenvectors for the following matrix (8)

$$\begin{bmatrix} 1 & 0 & -2 \\ 0 & 5 & 0 \\ -2 & 0 & 4 \end{bmatrix}$$

ii. Find a 3 × 3 orthogonal matrix $\boldsymbol{S}$ and a 3 × 3 diagonal matrix $\boldsymbol{D}$ such that $\boldsymbol{A = SDS^T}$.

13 a) A skier is on a mountain with equation $z = 100 - 0.4x^2 - 0.3y^2$, where z denotes height. (8)

i. The skier is located at the point with xy-coordinates **(1 , 1)**, and wants to ski downhill along the steepest possible path. In which direction (indicated by a vector **(a , b**) in the xy-plane) should the skier begin skiing.

ii. The skier begins skiing in the direction given by the xy-vector (**a , b)** you found in part (i), so the skier heads in a direction in space given by the vector **(a , b , c**). Find the value of **c**.

b) Find the linear approximation to the function $\boldsymbol{f(x,y) = 2 - \sin(-x - 3y)}$ at the point **(0 , π)**, and then use your answer to estimate $\boldsymbol{f(0.001 , \pi)}$. (6)

OR

14 a) Let ***g*** be the function given by (8)

$$g(x, y) = \begin{cases} \dfrac{x^2 y}{x^2 + y^2} & \text{if } (x, y) \neq (0,0); \\ 0 & \text{if } (x, y) = (0,0). \end{cases}$$

i. Calculate the partial derivatives of ***g*** at **(0 , 0)**.

ii. Show that ***g*** is not differentiable at **(0 , 0)**.

b) Find the second order Taylor series expansion for $f(x,y) = e^{-(x2+y2)} \cos(xy)$ about **(0 , 0)**. (6)

15 a) There are two bags. The first bag contains four mangos and two apples; the second bag contains four mangos and four apples. We also have a biased coin, which shows “heads” with probability 0.6 and “tails” with probability 0.4. If the coin shows “heads”. we pick a fruit at random from bag 1; otherwise we pick a fruit at random from bag 2. Your friend flips the coin (you cannot see the result), picks a fruit at random from the corresponding bag, and presents you a mango. (6)

What is the probability that the mango was picked from bag 2?

b) Suppose that one has written a computer program that sometimes compiles and sometimes not (code does not change). You decide to model the apparent stochasticity (success vs. no success) ***x*** of the compiler using a Bernoulli distribution with parameter μ: (8)

$$p(x \mid \mu) = \mu^x (1 - \mu)^{1-x}, \quad x \in \{0, 1\}$$

Choose a conjugate prior for the Bernoulli likelihood and compute the posterior distribution $p(\mu \mid x_1, \ldots, x_N)$.

OR

16 a) Consider a mixture of two Gaussian distributions (8)

$$0.4\mathcal{N}\left(\begin{bmatrix}10\\2\end{bmatrix},\begin{bmatrix}1&0\\0&1\end{bmatrix}\right)+0.6\mathcal{N}\left(\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}8.4&2.0\\2.0&1.7\end{bmatrix}\right)$$

i. Compute the marginal distributions for each dimension.

ii. Compute the mean, mode and median for each marginal distribution.

iii. Compute the mean and mode for the two-dimensional distribution.

b) Express the Binomial distribution as an exponential family distribution. Also express the Beta distribution is an exponential family distribution. Show that the product of the Beta and the Binomial distribution is also a member of the exponential family. (6)

17 a) Find the extrema of $\boldsymbol{f(x,y,z) = x - y + z}$ subject to $\boldsymbol{g(x,y,z) = x^2 + y^2 + z^2 = 2}$. (8)

b) Let

$$P=\begin{bmatrix}13&12&-2\\12&17&6\\-2&6&12\end{bmatrix},\ q=\begin{bmatrix}-22.0\\-14.5\\13.0\end{bmatrix},\ \text{and}\ r=1.$$

Show that $\boldsymbol{x^*} = \mathbf{(1\ ,\ 1/2\ ,\ -1)}$ is optimal for the optimization problem

$$\begin{array}{ll}\min & \frac{1}{2}x^{\mathsf{T}}Px+q^{\mathsf{T}}x+r\\ \text{s.t.} & -1\le x_i\le 1,\ i=1,2,3.\end{array}$$

(6)

OR

18 a) Derive the gradient descent training rule assuming that the target function is represented as $\boldsymbol{o_d = w_0 + w_1x_1 + \ldots + w_nx_n}$. Define explicitly the cost/ error function $\boldsymbol{E}$, assuming that a set of training examples $\boldsymbol{D}$ is provided, where each training example $\boldsymbol{d \in D}$ is associated with the target output $\boldsymbol{t_d}$. (8)

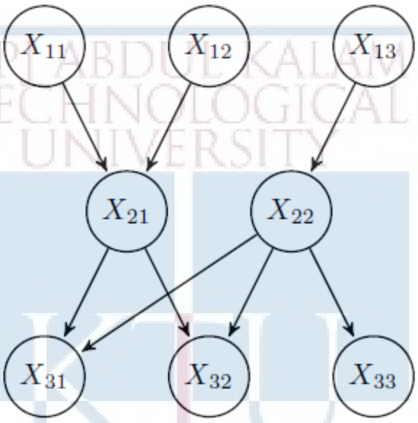
b) Find the maximum value of ***f(x,y,z) = xyz*** given that ***g(x,y,z) = x + y + z = 3*** and ***x,y,z >= 0***. (6)

19 a) Consider the following probability distribution (7)

$$P_\theta(x) = 2\theta x e^{-\theta x^2}$$

where $\boldsymbol{\theta}$ is a parameter and $\boldsymbol{x}$ is a positive real number. Suppose you get ***m*** i.i.d. samples $\boldsymbol{x_i}$ drawn from this distribution. Compute the maximum likelihood estimator for $\boldsymbol{\theta}$ based on these samples.

b) Consider the following Bayesian network with boolean variables. (7)



i. List variable(s) conditionally independent of X_{33} given $\boldsymbol{X_{11}}$ and $\boldsymbol{X_{12}}$

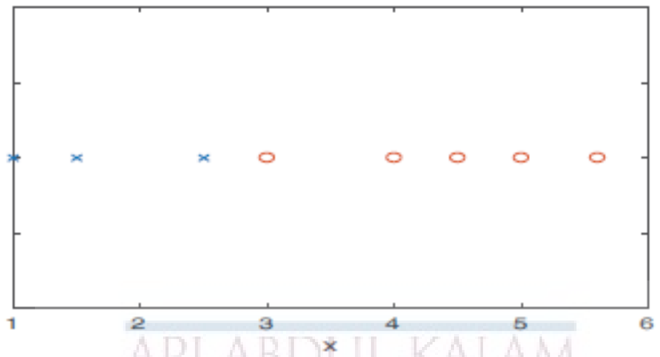
ii. List variable(s) conditionally independent of X_{33} and $\boldsymbol{X_{22}}$

iii. Write the joint probability $\boldsymbol{P(X_{11}, X_{12}, X_{13}, X_{21}, X_{22}, X_{31}, X_{32}, X_{33})}$ factored according to the Bayes net. How many parameters are necessary to define the conditional probability distributions for this Bayesian network?

iv. Write an expression for $\boldsymbol{P(X_{13} = 0, X_{22} = 1, X_{33} = 0)}$ in terms of the conditional probability distributions given in your answer to part (iii). Justify your answer.

OR

20 a) Consider the following one dimensional training data set, ’x’ denotes negative examples and ’o’ positive examples. The exact data points and their labels are given in the table below. Suppose a SVM is used to classify this data. (6)



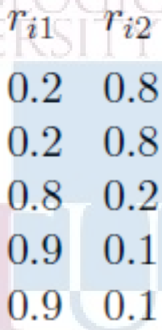
x	1	1.5	2.5	3	4	4.5	5	5.6
y	-1	-1	-1	1	1	1	1	1

i. Indicate which are the support vectors and mark the decision boundary.

ii. Give the value of the cost function and the model parameter after training.

b) Suppose that we are fitting a Gaussian mixture model for data items consisting of a single real value, ***x***, using ***K = 2*** components. We have ***N* = *5*** training cases, in which the values of ***x*** are as **5, 15, 25, 30, 40**. Using the EM algorithm to find the maximum likeihood estimates for the model parameters, what are the mixing proportions for the two components, π_1 and π_2, and the means for the two components, μ_1 and μ_2. The standard deviations for the two components are fixed at 10. (8)

Suppose that at some point in the EM algorithm, the **E** step found that the responsibilities of the two components for the five data items were as follows:



r_{i1}	r_{i2}
0.2	0.8
0.2	0.8
0.8	0.2
0.9	0.1
0.9	0.1

What values for the parameters π_1, π_2, μ_1, and μ_2 will be found in the next **M** step of the algorithm?

****

Teaching Plan

No	Topic	No. of Lectures (45)
1	**Module-I (LINEAR ALGEBRA)**	**8**
1.	Systems of Linear Equations – Matrices, Solving Systems of Linear Equations. Vector Spaces - Linear Independence.	1
2.	Vector Spaces - Basis and Rank	1
3.	Linear Mappings	1
4.	Norms, Inner Products, Lengths and Distances, Angles and Orthogonality, Orthonormal Basis, Orthogonal Complement	1
5.	Orthogonal Projections, Matrix Decompositions, Determinant and Trace.	1
6.	Eigenvalues and Eigenvectors	1
7.	Cholesky Decomposition, Eigen decomposition and Diagonalization	1
8.	Singular Value Decomposition - Matrix Approximation	1
	Module-II (VECTOR CALCULUS)	**6**
1	Differentiation of Univariate Functions, Partial Differentiation and Gradients	1
2	Gradients of Vector Valued Functions, Gradients of Matrices	1
3	Useful Identities for Computing Gradients	1
4	Backpropagation and Automatic Differentiation	1
5	Higher Order Derivatives	1
6	Linearization and Multivariate Taylor Series	1
3	**Module-III (Probability and Distributions)**	**10**
1	Construction of a Probability Space - Discrete and Continuous Probabilities (Lecture 1)	1

2	Construction of a Probability Space - Discrete and Continuous Probabilities (Lecture 2)	1
3	Sum Rule, Product Rule	1
4	Bayes' Theorem	1
5	Summary Statistics and Independence	1
6	Important probability Distributions (Lecture 1)	1
7	Important probability Distributions (Lecture 2)	1
8	Conjugacy and the Exponential Family (Lecture 1)	1
9	Conjugacy and the Exponential Family (Lecture 2)	1
10	Change of Variables/Inverse Transform	1
4	**Module-IV (Optimization)**	**7**
1	Optimization Using Gradient Descent.	1
2	Gradient Descent With Momentum, Stochastic Gradient Descent	1
3	Constrained Optimization and Lagrange Multipliers (Lecture 1)	1
4	Constrained Optimization and Lagrange Multipliers (Lecture 2)	1
5	Convex Optimization	1
6.	Linear Programming	1
7.	Quadratic Programming	1
5	**Module-V (CENTRAL MACHINE LEARNING PROBLEMS)**	**14**
1.	Data and Learning models - Empirical Risk Minimization,	1
2.	Parameter Estimation	1
3.	Directed Graphical Models	1
4.	Linear Regression	1
5.	Bayesian Linear Regression	1
6.	Maximum Likelihood as Orthogonal Projection	1
7.	Dimensionality Reduction with Principal Component Analysis - Maximum Variance Perspective, Projection Perspective.	1
8.	Eigenvector Computation and Low Rank Approximations	1
9.	Density Estimation with Gaussian Mixture Models	1

10.	Parameter Learning via Maximum Likelihood	1
11.	EM Algorithm	1
12.	Classification with Support Vector Machines - Separating Hyperplanes	1
13.	Primal Support Vector Machines, Dual Support Vector Machines	1
14.	Kernels	1
*Assignments may include applications of the above theory. With respect to module V, programming assignments may be given.		

CST 296	Principles of Program Analysis and Verification	Category	L	T	P	CREDIT	YEAR OF INTRODUCTION
		HONOURS	3	1	0	4	2019

Preamble: This is the foundational course for awarding B. Tech. Honours in Computer Science and Engineering with specialization in ***Formal Methods***. Program Analysis and Program Verification are two important areas of study, discussing Methods, Technologies and Tools to ensure reliability and correctness of software systems. The syllabus for this course is prepared with the view of introducing the Foundational Concepts, Methods and Tools in Program Analysis and Program Verification.

Prerequisite: Topics covered in the course Discrete Mathematical Structures (MAT 203).

Course Outcomes: After the completion of the course the student will be able to

CO1	Explain the concepts and results about Lattices, Chains, Fixed Points, Galois Connections, Monotone and Distributive Frameworks, Hoare Triples, Weakest Preconditions, Loop Invariants and Verification Conditions to perform Analysis and Verification of programs **(Cognitive knowledge level: Understand)**
CO2	Illustrate methods for doing intraprocedural/interprocedural Data flow Analysis for a given Program Analysis problem **(Cognitive knowledge level: Analyse)**
CO3	Formulate an Abstract Interpretation framework for a given Data flow Analysis problem and perform the analysis using the tool WALA **(Cognitive knowledge level: Analyse)**
CO4	Use Kildall's Algorithm to perform Abstract Interpretation of Programs and compare the results obtained by the Algorithm on Monotone and Distributive Frameworks **(Cognitive knowledge level: Apply)**
CO5	Explain the concept of Loop Invariants and use them in Hoare Triple based Weakest Precondition analysis to verify the total correctness of a code segment **(Cognitive knowledge level: Apply)**
CO6	Use the tool VCC to specify and verify the correctness of a C Program with respect to a given set of properties **(Cognitive knowledge level: Analyse)**

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✓	✓	✓	✓		✓				✓		✓
CO2	✓	✓	✓	✓		✓				✓		✓
CO3	✓	✓	✓	✓	✓	✓						✓
CO4	✓	✓	✓	✓		✓						✓
CO5	✓	✓	✓	✓		✓				✓		✓
CO6	✓	✓	✓	✓	✓	✓						✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern:

Bloom's Category	Continuous Assessment Tests		End Semester Examination Marks
	Test 1 (Percentage)	Test 2 (Percentage)	
Remember	30	30	30
Understand	30	30	30
Apply	40	40	40
Analyze			
Evaluate			
Create			

Mark Distribution

Total Marks	CIE Marks	ESE Marks	ESE Duration
150	**50**	**100**	**3 hours**

Continuous Internal Evaluation Pattern:

Attendance : 10 Marks

Continuous Assessment Tests : 25 Marks

Assignment : 15 Marks

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks

First series test shall be preferably conducted after completing the first half of the syllabus and the second series test shall be preferably conducted after completing the remaining part of the syllabus.

There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly covered module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly covered module), each with 7 marks. Out of the 7 questions in Part B, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions from Part A. Part B contains 2 questions from each module of which a student should answer any one, each question carries 14 marks. Each question in part B can have a maximum 2 sub-divisions.

SYLLABUS

Module 1

Mathematical Foundations – Partially Ordered Set, Complete Lattice, Construction of Complete Lattices, Chains, Fixed Points, Knaster-Tarski Fixed Point Theorem.

Module 2

Introduction to Program Analysis – The WHILE language, Reaching Definition Analysis, Data Flow Analysis, Abstract Interpretation, Algorithm to find the least solutions for the Data Flow Analysis problem.

Module 3

Intraprocedural DataFlow Analysis – Available Expressions Analysis, Reaching Definitions Analysis, Very Busy Expressions Analysis, Live Variable Analysis, Derived Data Flow Information, Monotone and Distributive Frameworks, Equation Solving - Maximal Fixed Point (MFP) and Meet Over all Paths (MOP) solutions.

Interprocedural Data Flow Analysis - Structural Operational Semantics, Intraprocedural versus Interprocedural Analysis, Making Context Explicit, Call Strings as Context, Flow Sensitivity versus Flow Insensitivity, Implementing Interprocedural Data-flow Analysis using the Tool WALA.

Module 4

Abstract Interpretation - A Mundane Approach to Correctness, Approximations of Fixed Points, Galois Connections, Systematic Design of Galois Connections, Induced Operations, Kildall's Algorithm for Abstract Interpretation.

Module 5

Program Verification - Why should we Specify and Verify Code, A framework for software verification - A core programming Language, Hoare Triples, Partial and Total Correctness, Program Variables and Logical Variables, Proof Calculus for Partial Correctness, Loop Invariants, Verifying code using the tool VCC (Verifier for Concurrent C).

Text Books

1. Flemming Nielson, Henne Nielson and Chris Kankin, Principles of Program Analysis, Springer (1998).
2. Michael Hutch and Mark Ryan, Logic in Computer Science - Modeling and Reasoning about Systems, Cambridge University Press, Second Edition.

References

1. Julian Dolby and Manu Sridharan, Core WALA Tutorial (PLDI 2010), available online at http://wala.sourceforge.net/files/PLDI_WALA_Tutorial.pdf

2. Ernie & Hillebrand, Mark & Tobies, Stephan (2012), Verifying C Programs: A VCC Tutorial.

Sample Course Level Assessment Questions

Course Outcome1 (CO1):

1. Find a lattice to represent the data states of a given program and propose a sound abstract interpretation framework to do a given analysis on the program.
2. When is an abstract interpretation framework said to be sound? Illustrate with an example.
3. When is an abstract interpretation framework said to be precise? Illustrate with an example.

Course Outcome2 (CO2):

1. Illustrate how one can do Intraprocedural Available Expression Analysis on a program.
2. Illustrate how one can do Intraprocedural Reaching Definition Analysis on a program.
3. Illustrate how one can do Intraprocedural Live Variable Analysis on a program.

Course Outcome3 (CO3):

1. Illustrate how one can do Interprocedural Data Flow Analysis using the tool WALA.

Course Outcome4 (CO4):

1. Illustrate the working of Kildall's algorithm to do Intraprocedural Available Expression Analysis on a program.
2. Compare the results obtained by applying Kildall's algorithms for Abstract Interpretation in Monotone and Distributive Frameworks.

Course Outcome5 (CO5):

1. Illustrate the process of obtaining verification conditions (VCs) using weakest precondition analysis.
2. Explain the concepts of partials and total correctness of programs.
3. Explain the necessity of obtaining loop invariants in verifying the total correctness of a program.

Course Outcome6 (CO6):

1. Using the tool VCC prove that a given code segment satisfies a given property.

Model Question paper

QP CODE: **PAGES:3**

Reg No:______________ **Name :______________**

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

4th SEMESTER B.TECH DEGREE (HONOURS) EXAMINATION, MONTH & YEAR

Course Code: CST 296

Course Name: Principles of Program Analysis and Verification

Max.Marks:100 **Duration: 3 Hours**

PART A

Answer all Questions. Each question carries 3 Marks

1. What is a complete lattice? Give an example of a complete lattice.
2. Show that every chain is a lattice.
3. Write a program in *while* language to find the factorial of a number. Explain the statements of your program.
4. Consider a program that calculates x^y through repeated multiplications. Draw the flow graph of the program.
5. What is Available Expression (AE) analysis? Give an application for AE analysis.
6. What is Live variable (LV) analysis? Give an application for LV analysis.
7. Let P be a program analysis problem (like LV, AE etc.) and (A, F_A, γ_{AC}) and (B, F_B, γ_{BC}) be two abstract interpretations such that B is more abstract than A. Let α and γ be the abstraction and concretization functions between A and B. Then, what are the conditions required for α and γ to form a Galois Connection?
8. When is Kildall's algorithm for abstract interpretation guaranteed to terminate? Justify your answer.
9. Is it possible to verify total correctness of a program using Hoare Logic? If yes, how is it possible?
10. Define *loop invariant*. Show a simple loop with a *loop invariant*.

PART B

Answer any one Question from each module. Each question carries 14 Marks

11.

a. What is an infinite ascending chain in a lattice? Show an example lattice with an infinite ascending chain. Is it possible for a complete lattice to contain an infinite ascending chain? **(7 marks)**

b. State and prove Knaster-Tarski fixed point theorem. **(7 marks)**

OR

12.

a. Consider the lattice $(\mathbb{N}, \leq)$. Let $f : \mathbb{N} \rightarrow \mathbb{N}$, be a function defined as follows: when $x < 100, f(x) = x + 1$, when $x > 100, f(x) = x - 1$, otherwise $f(x) = x$. Then, show the following for f: (i) the set of all fixpoints, (ii) the set of all pre-fixpoints and (iii) the set of all post-fixpoints. **(7 marks)**

b. Let $(D, \leq)$ be a lattice with a least upper bound for each subset of D. Then, prove that every subset of D has a greatest lower bound. **(7 marks)**

13.

a. With a suitable example, explain the equational approach in Data Flow Analysis. **(7 marks)**

b. With a suitable example, explain how you obtain the collecting semantics of a program point. **(7 marks)**

OR

14.

a. With an example, explain the Constrained Based Approach in Data Flow Analysis. **(7 marks)**

b. Discuss the properties of an algorithm to solve the problem of computing the least solution to the program analysis problems in Data Flow Analysis. **(7 marks)**

15.

a. Using Intraprocedural Reaching Definition Analysis, find the assignments killed and generated by each of the blocks in the program

```
[x:=5]^1;
[y:=1]^2;
while [x>1]^3 do
      ([y:=x*y]^4; [x:=x-1]^5)
```

(7 marks)

b. Analyse the following program using Intraprocedural Very Busy Expression analysis

```
if $[a>b]^1$ then
      ($[x:=b-a]^2$ ; $[y:=a-b]^3$)
else
      ($[y:=b-a]^4$; $[x:=a-b]^5$)
```

(7 marks)

OR

16.

a. Find Maximal Fixed Point (MFP) solution for the program

```
$[x:=a+b]^1$;
$[y:=a*b]^2$ ;
while $[y>a+b]^3$ do
      ($[a:=a+1]^4$; $[x:=a+b]^5$)
```

(7 marks)

b. With examples, explain the difference between flow sensitive and flow insensitive analysis. **(7 marks)**

17.

a. Prove that (L, α, γ, M) is an adjunction if and only if (L, α, γ, M) is a Galois connection. **(7 marks)**

b. Prove that if $\alpha : L \to M$ is completely additive then there exists $\gamma : M \to L$ such that (L, α, γ, M) is a Galois connection. Similarly, if $\gamma : M \to L$ is completely multiplicative then there exists $\alpha : L \to M$ such that (L, α, γ, M) is a Galois connection. **(7 marks)**

OR

18.

a. Show that if (L_i, α_i, γ_i, M_i) are Galois connections and β_i : V_i ➡ L_i are representation functions then

$$((\alpha_1 \circ \beta_1) \twoheadrightarrow (\alpha_2 \circ \beta_2)) (\rightarrow) = \alpha_2 \circ ((\beta_1 \twoheadrightarrow \beta_2) (\rightarrow)) \circ \gamma_1$$

(7 marks)

b. Briefly explain Kildall's algorithm for abstract interpretation **(7 marks)**

19.

a. Briefly explain the need of specification and verification of code. **(7 marks)**

b. Argue that Hoare Logic is sound. When Hoare Logic is complete? Let {A}P{B} be a Hoare triple such that Hoare Logic is complete for the program P. Then, is it always possible to check the validity of the Hoare Triple? If not, what is the difficulty? **(7 marks)**

OR

20.

a. With suitable examples, show the difference between partial and total correctness. **(7 marks)**

b. With a suitable example, show how a basic program segment can be verified using the tool VCC. **(7 marks)**

Teaching Plan

Module 1 (Mathematical Foundations)		6 Hours
1.1	Partially Ordered Set	1 Hour
1.2	Complete Lattice, Construction of Complete Lattices	1 Hour
1.3	Chains	1 Hour
1.4	Fixed Points	1 Hour
1.5	Knaster-Tarski Fixed Point Theorem	1 Hour
1.6	Proof of Knaster-Tarski Fixed Point Theorem	1 Hour
Module 2 (Introduction to Program Analysis)		**5 Hours**
2.1	The WHILE language	1 Hour
2.2	Data Flow Analysis	1 Hour
2.3	Reaching Definition Analysis	1 Hour
2.4	Abstract Interpretation	1 Hour
2.5	Algorithm to find the least solutions for the Data Flow Analysis problem	1 Hour
Module 3 (Data flow Analysis)		**15 Hours**
3.1	Available Expressions Analysis, Reaching Definitions Analysis	1 Hour
3.2	Very Busy Expressions Analysis	1 Hour
3.3	Live Variable Analysis	1 Hour
3.4	Derived Data Flow Information	1 Hour
3.5	Monotone and Distributive Frameworks	1 Hour
3.6	Equation Solving - MFP Solution	1 Hour

3.7	Equation Solving - MOP Solution	1 Hour
3.8	Structural Operational Semantics (Lecture 1)	1 Hour
3.9	Structural Operational Semantics (Lecture 2)	1 Hour
3.10	Intraprocedural versus Interprocedural Analysis	1 Hour
3.11	Making Context Explicit	1 Hour
3.12	Call Strings as Context	1 Hour
3.13	Flow Sensitivity versus Flow Insensitivity	1 Hour
3.14	Implementing Interprocedural Dataflow Analysis using the Tool WALA (Lecture 1)	1 Hour
3.15	Implementing Interprocedural Dataflow Analysis using the Tool WALA (Lecture 2)	1 Hour
Module 4 (Abstract Interpretation)		**8 Hours**
4.1	A Mundane Approach to Correctness	1 Hour
4.2	Approximations of Fixed Points	1 Hour
4.3	Galois Connections,	1 Hour
4.4	Systematic Design of Galois Connections (Lecture 1)	1 Hour
4.5	Systematic Design of Galois Connections (Lecture 2)	1 Hour
4.6	Induced Operations	1 Hour
4.7	Kildall’s Algorithm for Abstract Interpretation (Lecture 1)	1 Hour
4.8	Kildall’s Algorithm for Abstract Interpretation (Lecture 2)	1 Hour
Module 5 (Program Verification)		**11 Hours**
5.1	Why should we Specify and Verify Code	1 Hour
5.2	A framework for software verification - A core programming Language	1 Hour

5.3	Hoare Triples (Lecture 1)	1 Hour
5.4	Hoare Triples (Lecture 2)	1 Hour
5.5	Partial and Total Correctness	1 Hour
5.6	Program Variables and Logical Variables	1 Hour
5.7	Proof Calculus for Partial Correctness	1 Hour
5.8	Loop Invariants	1 Hour
5.9	Verifying C programs using the tool VCC (Lecture 1)	1 Hour
5.10	Verifying C programs using the tool VCC (Lecture 2)	1 Hour
5.11	Verifying C programs using the tool VCC (Lecture 3)	1 Hour

CST 393	CRYPTOGRAPHIC ALGORITHMS	Category	L	T	P	Credit	Year of Introduction
		VAC	3	1	0	4	2019

Preamble:

The course on Cryptographic Algorithms aims at exploring various algorithms deployed in offering confidentiality, integrity, authentication and non-repudiation services. This course covers classical encryption techniques, symmetric and public key crypto-system, key exchange and management, and authentication functions. The concepts covered in this course enable the learners in effective use of cryptographic algorithms for real life applications.

Prerequisite: A sound background in Number Theory**.**

Course Outcomes: After the completion of the course the student will be able to

CO1	Identify the security services provided for different types of security attacks. (**Cognitive Knowledge Level : Understand**)
CO2	Summarize the classical encryption techniques for information hiding. (**Cognitive Knowledge Level: Apply**)
CO3	Illustrate symmetric / asymmetric key cryptographic algorithms for secure communication.(**Cognitive Knowledge Level: Apply**)
CO4	Interpret key management techniques for secure communication.(**Cognitive Knowledge Level: Understand)**
CO5	Summarize message authentication functions in a secure communication scenario.(**Cognitive Knowledge Level: Understand**)

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1	✓	✓	✓									✓

CO2	✓	✓	✓		✓	✓						✓
CO3	✓	✓	✓	✓	✓	✓						✓
CO4	✓	✓	✓	✓	✓	✓						✓
CO5	✓	✓	✓	✓	✓	✓						✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**		**End Semester Examination Marks**
	Test1 (Percentage)	**Test2 (Percent**	

		age)	
Remember	30	30	30
Understand	30	30	30
Apply	40	40	40
Analyze			
Evaluate			
Create			

Mark Distribution

Total Marks	CIE Marks	ESE Marks	ESE Duration
150	50	100	3 hours

Continuous Internal Evaluation Pattern:

Attendance	: **10 marks**
Continuous Assessment Tests	: **25 marks**
Continuous Assessment Assignment	: **15 marks**

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks.

First Internal Examination shall be preferably conducted after completing the first half of the syllabus and the Second Internal Examination shall be preferably conducted after completing remaining part of the syllabus.

There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly covered module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly covered module), each with 7 marks. Out of the 7 questions in Part B, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which a student should answer any one. Each question can have maximum 2 sub-divisions and carries 14 marks.

Syllabus

Module-1 (Introduction to the Concepts of Security)

Need for security, Security approaches, Principles of security, Types of attacks, OSI Security Architecture, Classical encryption techniques - Substitution techniques, Transposition techniques. Stream cipher, Block cipher, Public key cryptosystems vs. Symmetric key cryptosystems, Encrypting communication channels.

Module-2 (Symmetric Key Cryptosystems)

Overview of symmetric key cryptography, Block cipher principles, Data Encryption Standard (DES), Differential and Linear cryptanalysis, Double DES, Triple DES, International Data Encryption Algorithm (IDEA), Advanced Encryption Algorithm (AES),Block cipher modes of operation, Stream cipher, RC4.

Module-3 (Public Key Cryptosystems)

Principles of public key cryptosystems, RSA algorithm, RSA illustration, Attacks, ElGamal cryptographic system, Knapsack algorithm, Diffie-Hellman key exchange algorithm, Elliptical curve cryptosystems.

Module-4 (Key Management)

Symmetric key distribution using symmetric encryption, Symmetric key distribution using asymmetric encryption, Distribution of public keys, Generating keys, transferring keys, Verifying keys, Updating keys, Storing keys, Backup keys, Compromised keys, Public key infrastructure.

Module – 5 (Authentication)

Authentication requirements, Authentication functions, Message authentication codes (MAC), Hash functions, Security of Hash functions and MAC, Message Digest 5 (MD5), Secure Hash Algorithm (SHA)-512, Hash-based Message Authentication Code (HMAC), Cipher-based Message Authentication Code (CMAC), X.509 Authentication services.

Text Books

1. William Stallings, Cryptography and Network Security Principles and Practice, Pearson Edu, 6e.
2. Bruice Schneier, Applied Cryptography Protocols, Algorithms and source code in C, Wiley,2e.

References

1. Behrouz A. Forouzan, Cryptography and Network Security, McGraw Hill, 2e.

2. Johannes A. Buchmann, Introduction to Cryptography, Springer, 2e.

3. DouglasR. Stinson, Cryptography Theory and Practice, 3e,Chapman & Hall/CRC, 2006.

4. Bernard Menezes, Network Security and Cryptography, Cengage Learning, 2011.

Sample Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.

2. Discuss the different security services provided for preventing security attacks.

Course Outcome 2 (CO2):

1. The encryption key in a transposition cipher is (3,2,6,1,5,4). Find the decryption key

2.Discuss the process of encryption in Vernam cipher

Course Outcome 3 (CO3):

1. Devise a meet-in-the-middle attack for a triple DES.

2. Write an algorithm for the InvSubBytes transformation and implement using python (**Assignment**)
3. Consider the following elliptic curve signature scheme. We have a global elliptic curve, prime *p*, and "generator" G. Alice picks a private signing key X_A and forms the public verifying $Y_A = X_AG$. To sign a message *M*:
    - Alice picks a value k
    - Alice sends Bob *M*, k and the signature $S = M - kX_AG$.
    - Bob verifies that $M=S+kY_A$.

   Show that the verification process produces an equality if the signature is valid.
4. Write an algorithm to add two points on an elliptic curve over GF(*p*) and implement using Python. **(Assignment)**
5. Write an algorithm for encryption using knapsack cryptosystem and implement using Java. **(Assignment)**

Course Outcome4 (CO4):

1. List four general categories of schemes for the distribution of public keys.
2. What are the essential ingredients of a public-key directory?

Course Outcome 5 (CO5):

1. State the value of the length field in SHA-512 if the length of the message is 1919 bits and 1920 bits.
2. Write an algorithm in pseudo code for HMAC and implement using Python (**Assignment**)

Model Question Paper

QP CODE:
Reg No:______________
Name :______________ **PAGES : 3**

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIFTH SEMESTER B.TECH DEGREE EXAMINATION(HONORS), MONTH & YEAR

Course Code: CST 393

Course Name: Cryptographic Algorithms

Max.Marks:100 **Duration: 3 Hours**

PART A

Answer all Questions. Each question carries 3 Marks

1. State the two approaches in attacking a cipher.

2. Define Substitution Cipher. Encrypt using one time pad M = HONORS and K = CIPHER.

3. Specify the purpose of S-Boxes in Data Encryption Standard (DES).

4. Differentiate between diffusion and confusion.

5. Perform encryption using RSA Algorithm for the following p=7; q=11; e=13; M=5.

6. Is Diffie-Hellman key exchange protocol vulnerable? Justify.

7. List the techniques for distribution of public keys.

8. Define a certificate authority and its relation to public key cryptography.

9. Distinguish between integrity and message authentication.

10. What types of attacks are addressed by message authentication?

(10x3=30)

Part B

(Answer any one question from each module. Each question carries 14 Marks)

11. (a) With a neat sketch, Explain OSI Security architecture model. **(8)**

(b) How does link encryption differ from end-to-end encryption? Explain. **(6)**

OR

12. (a) Encrypt the text "cryptography" using the Hill Cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show the calculations. **(8)**

(b) Illustrate the steps involved in encrypting a plain text using playfair cipher with an example. **(6)**

13. (a) With a neat sketch, explain a single round in DES. **10**

(b) Explain encryption and decryption using 2 keys and 3 keys of triple DES. **(4)**

OR

14. (a) Explain the block cipher modes i) Cipher feedback mode ii) Output feedback mode. **(8)**

(b) Describe the four types of transformations in AES. **(6)**

15. (a) Write an algorithm for generating public and private key using Elliptical curve cryptography. **(10)**

(b) The equation $y^2=x^3 +x+1$, the calculation is done modulo 13. Add two points R= P+Q, where P= (4,2) and Q= (10,6). **(4)**

OR

16. User A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and primitive root alpha=7.

(a) If user A has private key X_A =3, What is A's public key Y_A? **(7)**

(b) If user B has private key X_B =6, What is A's public key $Y_{\mathbf{B}}$? **(7)**

17. (a) Define a session key and show how a KDC can create can create a session key between Alice and Bob. **(7)**

(b) What are the requirements for the use of a public-key certificate scheme? **(7)**

OR

18. (a) What are the core components of a PKI? Briefly describe each component. **(8)**

(b) Describe the following (i) Updating keys (ii) Compromised Keys. **(6)**

19. (a) Describe how SHA-512 logic produce message digest **(10)**

(b) Distinguish between HMAC and CMAC **(4)**

OR

20. (a) Specify the format for X.509 certificate. Explain the steps required to obtain user's certificate. **(7)**

(b) With suitable block diagrams, explain the types of functions that may be used to produce an authenticator. **(8)**

Teaching Plan

No	Contents	No of Lecture Hrs
	Module - 1 (Introduction to the Concepts of Security) (9 hrs)	
1.1	Need for security, Security approaches	1 hour
1.2	Principles of security, Types of attacks	1 hour
1.3	OSI Security Architecture	1 hour
1.4	Classical encryption techniques: Substitution techniques(Caesar cipher, Monoalphabetic cipher, Playfair cipher)	1 hour
1.5	Classical encryption techniques: Substitution techniques (Hill cipher, Polyalphabetic cipher, One-time pad)	1 hour
1.6	Classical encryption techniques: Transposition techniques	1 hour
1.7	Stream cipher, Block cipher	1 hour
1.8	Public- key cryptosystems vs. Symmetric key cryptosystems	1 hour
1.9	Encrypting communication channels	1 hour
	Module - 2 (Symmetric key cryptosystems) (11 hrs)	
2.1	Overview of symmetric key cryptography	1 hour
2.2	Block cipher principles	1 hour
2.3	Data Encryption Standard (DES)	1 hour
2.4	DES design criteria	1 hour
2.5	Differential and Linear cryptanalysis	1 hour
2.6	Double DES, Triple DES	1 hour

2.7	IDEA	1 hour
2.8	Advanced Encryption Algorithm (AES structure)	1 hour
2.9	Advanced Encryption Algorithm (Transformations)	1 hour
2.10	Block cipher modes of operation	1 hour
2.11	Stream cipher, RC4	1 hour
Module - 3 (Public key cryptosystems) (8 hrs)		
3.1	Principles of public key cryptosystems	1 hour
3.2	RSA algorithm	1 hour
3.3	RSA illustration, Attacks	1 hour
3.4	ElGamal cryptographic system	1 hour
3.5	Knapsack algorithm	1 hour
3.6	Diffie-Hellman key exchange algorithm	1 hour
3.7	Elliptical curve cryptosystems(Elliptical curve arithmetic)	1 hour
3.8	Elliptical curve cryptosystems (Elliptical curve algorithm)	1 hour
Module - 4 (Key Management) (8 hrs) [Text book-2]		
4.1	Symmetric key distribution using symmetric encryption	1 hour
4.2	Symmetric key distribution using asymmetric encryption	1 hour
4.3	Distribution of public keys	1 hour
4.4	Generating keys, Transferring keys	1 hour

4.5	Verifying keys, Updating keys	1 hour
4.6	Storing keys, Backup keys	1 hour
4.7	Compromised keys	1 hour
4.8	Public key infrastructure	1 hour
Module - 5 (Authentication) (9 hrs)		
5.1	Authentication requirements	1 hour
5.2	Authentication functions	1 hour
5.3	Message Authentication Codes (MAC)	1 hour
5.4	Hash functions	1 hour
5.5	Security of Hash functions and MAC	1 hour
5.6	MD5	1 hour
5.7	SHA-512	1 hour
5.8	HMAC, CMAC	1 hour
5.9	X.509 Authentication services	1 hour

CST 394	NETWORK SECURITY	Category	L	T	P	Credits	Year of Introduction
		VAC	3	1	0	4	2019

Preamble:

The purpose of this course is to create a better understanding of the network security concepts. This course covers network security standards, email security services, web security mechanisms, firewalls and wireless security mechanisms. This course helps the learner to gain insight into the key aspects of secure network communication and enables to apply in real-life scenarios.

Prerequisite: A sound background in Number Theory and Cryptographic Algorithms.

Course Outcomes: After the completion of the course the student will be able to

CO#	Course Outcomes
CO1	Identify the key aspects of security, intrusion detection systems and digital signature schemes **(Cognitive Knowledge Level: Apply)**
CO2	Explain the security standards used in network communication **(Cognitive Knowledge Level:Understand)**
CO3	Identify the mechanisms in email security services **(Cognitive Knowledge Level: Apply)**
CO4	Summarize the protocols used to provide web security **(Cognitive Knowledge Level: Understand)**
CO5	Explain the fundamental concepts of wireless network security and firewalls **(Cognitive Knowledge Level: Understand)**

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✓	✓	✓	✓								✓
CO2	✓	✓	✓	✓								✓
CO3	✓	✓	✓	✓		✓						✓
CO4	✓	✓	✓	✓	✓	✓						✓
CO5	✓	✓	✓	✓								✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Lifelong learning

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**		**End Semester Examination (%)**
	Test 1 (%)	**Test 2 (%)**	
Remember	30	30	30
Understand	40	40	40
Apply	30	30	30
Analyze			
Evaluate			
Create			

Mark Distribution

Total Marks	CIE Marks	ESE Marks	ESE Duration
150	50	100	3

Continuous Internal Evaluation Pattern:

Attendance	**: 10 marks**
Continuous Assessment Tests	**: 25 marks**
Continuous Assessment Assignment	**: 15 marks**

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks. The first series test shall be preferably conducted after completing the first half of the syllabus and the second series test shall be preferably conducted after completing remaining part of the syllabus. There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly completed module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly completed module), each with 7 marks. Out of the 7 questions, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which a student should answer any one. Each question can have maximum 2 sub-divisions and carries 14 marks.

Syllabus

Module – 1 (Network Security Basics)

Introduction to network security - Security requirements, Challenges of security, Network security model. Malicious programs – Worms, Viruses, Trojans, Spyware, Adware. Intrusion Detection Systems (IDS) - Uses, Techniques. Digital signatures - ElGamal, Schnorr, Digital Signature Standard (DSS).

Module – 2 (Network Security Standards)

Kerberos v4 – Configuration, Authentication, Encryption, Message formats. Kerberos v5 – Cryptographic algorithms, Message formats. Public Key Infrastructure (PKI) – Trust models, Revocation. Real-time communication security – Perfect Forward Secrecy (PFS), Denial-of-Service protection, Endpoint identifier hiding, Live partner reassurance. Internet Protocol Security (IPSec) - Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE) phases.

Module – 3 (Email Security)

Introduction to email security - Security services for email, Establishing keys, Privacy, Authentication, Message integrity, Non-repudiation. Privacy Enhanced Mail (PEM) – Encryption, Source authentication and integrity protection, Message formats. Secure/Multipurpose Internet Mail Extensions (S/MIME) – Messages, Differences from PEM. Pretty Good Privacy (PGP) - Encoding, Certificate and key revocation, Anomalies, Object formats.

Module – 4 (Web Security)

Introduction to web security - Web security considerations, Threats. Secure Sockets Layer (SSL) – Architecture, Protocols, Transport Layer Security (TLS) – Differences from SSL. Hypertext Transfer Protocol Secure (HTTPS) – Connection initiation, Closure. Secure Shell (SSH) – Transport layer protocol, User authentication protocol, Connection protocol.

Module – 5 (Wireless Network Security and Firewalls)

IEEE 802.11 Wireless LAN - Network components, Architectural model, Services. IEEE 802.11i wireless LAN security - Services, Phases of operation. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, Wireless Application Protocol (WAP) – Services, Protocol architecture. Firewalls – Need for firewalls, Packet filters, Circuit-level firewalls, Application layer firewalls.

Text Books

1. C. Kaufman, R. Perlman and M. Speciner, “Network Security: Private Communication in a Public World”, 2/e, PHI.
2. William Stallings, “Cryptography and Network Security Principles and Practice”, 5/e, Pearson

Education Asia.

References

1. Behrouz A. Forouzan, Debdeep Mukhopadhyay, “Cryptography and Network Security”, 3/e, Tata McGraw Hill.
2. Tyler Wrightson, “Wireless Network Security A Beginner’s Guide”, 2012, Tata McGraw Hill.
3. William Stallings, “Network Security Essentials: Applications and Standards”, 4/e, Prentice Hall.
4. Schiller J., Mobile Communications, 2/e, Pearson Education.
5. Roberta Bragg et. al., “Network Security: The Complete Reference”, Tata McGraw Hill.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Using the Schnorr digital signature scheme, let q = 83, p = 997 and d = 23. Find values for e_1 and e_2.
2. The Digital Signature Algorithm (DSA) specifies that if the signature generation process results in a value of zero, a new value of k should be generated and the signature should be recalculated. Give reason.

Course Outcome 2 (CO2):

1. In Kerberos v4, the authenticator field is not of security benefit when asking the Key Distribution Center (KDC) for a ticket for Bob, but useful when logging in as Bob. Give reasons for your answer.
2. How does the stateless cookie protocol provide clogging protection?

Course Outcome 3 (CO3):

1. If Alice is sending an ENCRYPTED message, she first signs the message digest with her private key and then encrypts the message digest with the pre-message secret key. Why this last encryption was considered necessary for encrypted messages and not for MIC-CLEAR or MIC-ONLY?
2. Which security services are considered desirable in the following cases? (i) Sending a purchase order (ii) Sending a ransom note. (iii) Sending a mission description to security officials.
3. Explain the security mechanism used in Gmail communication.

Course Outcome 4 (CO4):

1. Is it possible in SSL for the receiver to reorder SSL record blocks that arrive out of order? If so, how it can be done? If not, why?
2. Describe any five web security threats, their consequences and countermeasures.

Course Outcome 5 (CO5):

1. Explain the security areas addressed by IEEE 802.11i.
2. Describe the advantages and disadvantages of application layer firewalls.

Model Question Paper

QP CODE:
Reg. No:______________
Name:________________ **PAGES : 3**

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SIXTH SEMESTER B.TECH. DEGREE (HONORS) EXAMINATION, MONTH &YEAR
Course Code: CST 394

Course Name: Network Security

Max.Marks:100 **Duration: 3 Hours**

PART A

Answer all Questions. Each question carries 3 Marks

1. Distinguish between signature-based and anomaly-based intrusion detection techniques.

2. A trusted third party is considered as a main component in a network security model. Why?

3. How is endpoint identifier hiding achieved in real-time communication?

4. Show how encryption is used to provide privacy and integrity in Kerberos v5.

5. End-to-end privacy is essential for e-mail security. How is this achieved?

6. List the four steps for preparing an EnvelopedData MIME entity.

7. Show the operation of a Secure Sockets Layer (SSL) Record protocol.

8. For Secure Shell (SSH) packets, what is the advantage of not including the MAC in the scope of packet encryption?

9. List the three security services provided by IEEE 802.11i.

10. Define the terms Access Point, Basic Service Set, Extended Service Set.

(10x3=30)

Part B

(Answer any one question from each module. Each question carries 14 Marks)

11. (a) Using the ElGamal scheme, let p = 881 and d = 700, find values for e1 and e2. Choose r = 17. Find the value of S1 and S2 if M = 400. **(8)**

(b) Explain the requirements and challenges of network security. **(6)**

OR

12. (a) In ElGamal, Schnorr and DSS, what happens if an attacker can find the value of random secret key used by the signer? Also, what happens if a user uses the same value of random secret key to sign two messages? Explain your answer for each scheme separately. **(8)**

(b) Explain the network security model with the help of a neat diagram. **(6)**

13. (a) Alice wishes to log into Bob's workstation remotely. List the steps involved in this communication if Kerberos v4 is used. **(7)**

(b) How does Diffie-Hellman technique provide perfect forward secrecy using signature keys? **(7)**

OR

14. (a) Explain the algorithm for Message Authentication Code (MAC) calculation and verification in Kerberos v5 rsa-md5-des. **(8)**

(b) Compare the aggressive mode and main mode of Phase 1 Internet Key Exchange (IKE). **(6)**

15. (a) Describe the different methods by which authentication of source is performed in email communication. **(7)**

(b) Explain the Signed data and Clear-signed data functions provided by S/MIME. **(7)**

OR

16. (a) Explain the advantages of Pretty Good Privacy (PGP) over Privacy Enhanced Mail (PEM). **(7)**

(b) Define non-repudiation. Describe the different ways by which it is implemented in email communication. **(7)**

17. (a) Describe the significance of pseudo-random function of Transport Layer Security. **(7)**

(b) Explain the four different phases of Secure Sockets Layer (SSL) HandshakeProtocol. **(7)**

OR

18. (a) Describe how connection initiation and connection closure is done in Hyper Text Transfer Protocol Secure (HTTPS). **(7)**

(b) Illustrate the sequence of events in Secure Shell (SSH) transport layer protocol packet exchanges. **(7)**

19. (a) Explain the Discovery phase and Authentication phase of IEEE 802.11i operation. **(7)**

(b) Why are firewalls needed? Compare the features of packet filters and circuit level firewalls. **(7)**

OR

20. (a) Explain the two authentication methods used in Wired Equivalent Privacy (WEP). **(7)**

(b) Describe the three transaction classes provided by Wireless Transaction Protocol. **(7)**

Teaching Plan

No	Contents	No of Lecture Hrs
Module - 1 (Network Security Basics) (7 hrs)		
1.1	Security requirements, Challenges of security	1
1.2	Network security model	1
1.3	Worms, Viruses, Trojans, Spyware, Adware	1
1.4	Intrusion Detection Systems (IDS) uses, Techniques	1
1.5	ElGamal digital signature	1
1.6	Schnorr digital signature	1
1.7	Digital Signature Standard (DSS)	1
Module - 2 (Network Security Standards) (12 hrs)		
2.1	Kerberos v4 configuration, Authentication	1
2.2	Kerberos v4 encryption	1
2.3	Kerberos v4 message formats	1
2.4	Kerberos v5 cryptographic algorithms – rsa-md5-des, des-mac, des-mac-k	1
2.5	Kerberos v5 cryptographic algorithms - rsa-md4-des, rsa-md4-des-k, Encryption for privacy and integrity	1
2.6	Kerberos v5 message formats	1
2.7	Public Key Infrastructure (PKI) trust models	1
2.8	PKI revocation	1
2.9	Perfect Forward Secrecy (PFS), Denial-of-Service protection	1
2.10	Endpoint identifier hiding, Live partner reassurance	1
2.11	Internet Protocol Security (IPSec) Authentication Header (AH), Encapsulating Security Payload (ESP)	1

2.12	Internet Key Exchange (IKE) phases	1
Module - 3 (Email Security) (9 hrs)		
3.1	Security services for email, Establishing keys, Privacy	1
3.2	Authentication, Message integrity, Non-repudiation	1
3.3	Privacy Enhanced Mail (PEM) encryption, Source authentication	1
3.4	PEM integrity protection, Message formats (Lecture 1)	1
3.5	PEM message formats (Lecture 2)	1
3.6	Secure/Multipurpose Internet Mail Extensions (S/MIME) – Messages, Differences from PEM	1
3.7	Pretty Good Privacy (PGP) encoding, Certificate and key revocation, Anomalies	1
3.8	PGP Object formats (Lecture 1)	1
3.9	PGP Object formats (Lecture 2)	1
Module – 4 (Web Security)(9 hrs)		
4.1	Web security considerations, Threats, Secure Sockets Layer (SSL) architecture	1
4.2	SSL protocols (Lecture 1)	1
4.3	SSL protocols (Lecture 2)	1
4.4	Transport Layer Security (TLS) differences from SSL (Lecture 1)	1
4.5	TLS differences from SSL (Lecture 2)	1
4.6	Hypertext Transfer Protocol Secure (HTTPS) connection initiation, Closure	1
4.7	Secure Shell (SSH) transport layer protocol	1
4.8	SSH user authentication protocol	1
4.9	SSH connection protocol	1

Module - 5 (Wireless Security and Firewalls) (8 hrs)		
5.1	IEEE 802.11 Wireless LAN network components, Architectural model, Services	1
5.2	IEEE 802.11i wireless LAN security services, Phases of operation (Lecture 1)	1
5.3	IEEE 802.11i phases of operation (Lecture 2)	1
5.4	Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2	1
5.5	Wireless Application Protocol (WAP) services, Protocol architecture (Lecture 1)	1
5.6	WAP protocol architecture (Lecture 2)	1
5.7	Need for firewalls, Packet filters	1
5.8	Circuit-level firewalls, Application layer firewalls	1

CST 395	NEURAL NETWORKS AND DEEP LEARNING	Category	L	T	P	Credit	Year of Introduction
		VAC	3	1	0	4	2019

Preamble:

Neural networks is a biologically inspired programming paradigm which enables a computer to learn from observational data and deep learning is a powerful set of techniques for training neural networks. This course introduces the key concepts in neural networks, its architecture and learning paradigms, optimization techniques, basic concepts in deep learning, Convolutional Neural Networks and Recurrent Neural Networks. The students will be able to provide best solutions to real world problems in domains such as computer vision and natural language processing.

Prerequisite: A Sound knowledge in Computational fundamentals of machine learning

Course Outcomes: After the completion of the course the student will be able to

CO1	Demonstrate the basic concepts of machine learning models and performance measures. **(Cognitive Knowledge Level : Understand)**
CO2	Illustrate the basic concepts of neural networks and its practical issues**(Cognitive Knowledge Level : Apply)**
CO3	Outline the standard regularization and optimization techniques for deep neural networks (**Cognitive Knowledge Level : Understand)**
CO4	Build CNN and RNN models for different use cases. **(Cognitive Knowledge Level : Apply)**
CO5	Explain the concepts of modern RNNs like LSTM, GRU **(Cognitive Knowledge Level : Understand)**

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✓	✓	✓	✓								✓
CO2	✓	✓	✓	✓								✓
CO3	✓	✓	✓	✓								✓
CO4	✓	✓	✓	✓	✓	✓						✓
CO5	✓	✓	✓	✓								✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		End Semester Examination Marks
	Test1 (%)	Test2 (%)	
Remember	30	30	30
Understand	40	40	40
Apply	30	30	30
Analyse			
Evaluate			
Create			

Mark Distribution

Total Marks	CIE Marks	ESE Marks	ESE Duration
150	50	100	3 hours

Continuous Internal Evaluation Pattern

Attendance	**10 marks**
Continuous Assessment Tests	**25 marks**
Continuous Assessment Assignment	**15 marks**

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks. First Internal Examination shall be preferably conducted after completing the first half of the syllabus and the Second Internal Examination shall be preferably conducted after completing the remaining part of the syllabus. There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly covered module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly covered module), each with 7 marks. Out of the 7 questions in Part B, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which a student should answer any one. Each question can have a maximum 2 subdivisions and carry 14 marks.

Syllabus

Module - 1 (Basics of Machine Learning)

Machine Learning basics - Learning algorithms - Supervised, Unsupervised, Reinforcement, Overfitting, Underfitting, Hyper parameters and Validation sets, Estimators -Bias and Variance. Challenges in machine learning. Simple Linear Regression, Logistic Regression, Performance measures - Confusion matrix, Accuracy, Precision, Recall, Sensitivity, Specificity, Receiver Operating Characteristic curve(ROC), Area Under Curve(AUC).

Module -2 (Neural Networks)

Introduction to neural networks -Single layer perceptrons, Multi Layer Perceptrons (MLPs), Representation Power of MLPs, Activation functions - Sigmoid, Tanh, ReLU, Softmax. Risk minimization, Loss function, Training MLPs with backpropagation, Practical issues in neural network training - The Problem of Overfitting, Vanishing and exploding gradient problems, Difficulties in convergence, Local and spurious Optima, Computational Challenges. Applications of neural networks.

Module 3 (Deep learning)

Introduction to deep learning, Deep feed forward network, Training deep models, Optimization techniques - Gradient Descent (GD), GD with momentum, Nesterov accelerated GD, Stochastic GD, AdaGrad, RMSProp, Adam. Regularization Techniques - L1 and L2 regularization, Early stopping, Dataset augmentation, Parameter sharing and tying, Injecting noise at input, Ensemble methods, Dropout, Parameter initialization.

Module -4 (Convolutional Neural Network)

Convolutional Neural Networks – Convolution operation, Motivation, Pooling, Convolution and Pooling as an infinitely strong prior, Variants of convolution functions, Structured outputs, Data types, Efficient convolution algorithms. Practical use cases for CNNs, Case study - Building CNN model AlexNet with handwritten digit dataset MNIST.

Module- 5 (Recurrent Neural Network)

Recurrent neural networks – Computational graphs, RNN design, encoder – decoder sequence to sequence architectures, deep recurrent networks, recursive neural networks, modern RNNs LSTM and GRU, Practical use cases for RNNs. Case study - Natural Language Processing.

Text Book

1. Goodfellow, I., Bengio,Y., and Courville, A., Deep Learning, MIT Press, 2016.
2. Neural Networks and Deep Learning, Aggarwal, Charu C., c Springer International Publishing AG, part of Springer Nature 2018
3. Fundamentals of Deep Learning: Designing Next-Generation Machine Intelligence Algorithms (1st. ed.). Nikhil Buduma and Nicholas Locascio. 2017. O'Reilly Media, Inc.

Reference Books

1. Satish Kumar, Neural Networks: A Classroom Approach, Tata McGraw-Hill Education, 2004.
2. Yegnanarayana, B., Artificial Neural Networks PHI Learning Pvt. Ltd, 2009.
3. Michael Nielsen, Neural Networks and Deep Learning, 2018

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Predict the price of a 1000 square feet house using the regression model generated from the following data.

No.	Square feet	Price(Lakhs)
1	500	5
2	900	10
3	1200	13
4	1500	18
5	2000	25
6	2500	32
7	2700	35

2. Consider a two-class classification problem of predicting whether a photograph contains a man or a woman. Suppose we have a test dataset of 10 records with expected outcomes and a set of predictions from our classification algorithm. Compute the confusion matrix, accuracy, precision, recall, sensitivity and specificity on the following data.

Sl.**No.**	Actual	Predicted
1	man	woman
2	man	man
3	woman	woman
4	man	man

5	man	woman
6	woman	woman
7	woman	man
8	man	man
9	man	woman
10	woman	woman

Course Outcome 2 (CO2):

1. Suppose you have a 3-dimensional input x = (x1, x2, x3) = (2, 2, 1) fully connected with weights (0.5, 0.3, 0.2) to one neuron which is in the hidden layer with sigmoid activation function. Calculate the output of the hidden layer neuron.
2. Consider the case of the XOR function in which the two points {(0, 0),(1, 1)} belong to one class, and the other two points {(1, 0),(0, 1)} belong to the other class. Design a multilayer perceptron for this binary classification problem.

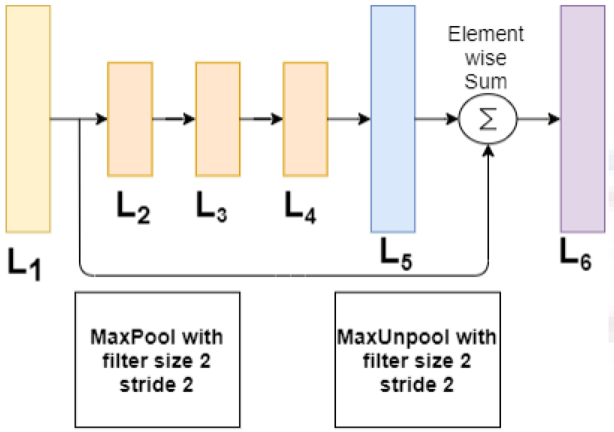
Course Outcome 3 (CO3):

1. Derive a mathematical expression to show L2 regularization as weight decay.
2. Explain how L2 regularization improves the performance of deep feed forward neural networks.
3. Explain how L1 regularization method leads to weight sparsity.

Course Outcome 4 (CO4):

1. Draw and explain the architecture of convolutional neural networks.
2. You are given a classification problem to classify the handwritten digits. Suggest a learning and/or inference machine with its architecture, an objective function, and an optimization routine, along with how input and output will be prepared for the classifier.
3. In a Deep CNN architecture the feature map L_1 was processed by the following operations as shown in the figure. First down sampled using max pool operation of size 2 and stride 2, and three convolution operations and finally max unpool operation and followed by an element wise sum. The feature map L_1 and L_4 are given below. Compute the matrix L6.

$$L_1 = \begin{matrix} 10 & 20 & 15 & 22 \\ 20 & 16 & 28 & 30 \\ 30 & 12 & 20 & 16 \\ 20 & 20 & 40 & 12 \end{matrix} \qquad L_4 = \begin{matrix} 10 & 20 \\ 20 & 30 \end{matrix}$$


Element wise Sum
Σ
L_1
L_2
L_3
L_4
L_5
L_6
MaxPool with filter size 2 stride 2
MaxUnpool with filter size 2 stride 2

4. Illustrate the workings of the RNN with an example of a single sequence defined on a vocabulary of four words.

Course Outcome 5 (CO5):

1. Draw and explain the architecture of LSTM.
2. List the differences between LSTM and GRU

Model Question Paper

QP CODE: **PAGES:4**

Reg No:_______________

Name:_________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIFTH SEMESTER B.TECH DEGREE EXAMINATION(HONORS), MONTH & YEAR

Course Code: CST 395

Course Name: Neural Networks and Deep Learning

Max.Marks:100 **Duration:3 Hours**

PART A

Answer all Questions. Each question carries 3 Marks

1. List and compare the types of machine learning algorithms

2. Suppose 10000 patients get tested for flu; out of them, 9000 are actually healthy and 1000 are actually sick. For the sick people, a test was positive for 620 and negative for 380. For healthy people, the same test was positive for 180 and negative for 8820. Construct a confusion matrix for the data and compute the

accuracy, precision and recall for the data

3. Illustrate the limitation of a single layer perceptron with an example

4. Specify the advantages of ReLU over sigmoid activation function.

5. Derive weight updating rule in gradient descent when the error function is a) mean squared error b) cross entropy

6. List any three methods to prevent overfitting in neural networks

7. What happens if the stride of the convolutional layer increases? What can be the maximum stride? Justify your answer.

8. Consider an activation volume of size 13×13×64 and a filter of size 3×3×64. Discuss whether it is possible to perform convolutions with strides 2, 3 and 5. Justify your answer in each case.

9. How does a recursive neural network work?

10. List down three differences between LSTM and RNN

(10x3=30)

Part B

(Answer any one question from each module. Each question carries 14 Marks)

11. (a) Prove that the decision boundary of binary logistic regression is linear **(9)**

(b) Given the following data, construct the ROC curve of the data. Compute the AUC. **(5)**

Threshold	**TP**	TN	FP	FN
1	0	25	0	29
2	7	25	0	22
3	18	24	1	11
4	26	20	5	3
5	29	11	14	0

6	29	0	25	0
7	29	0	25	0

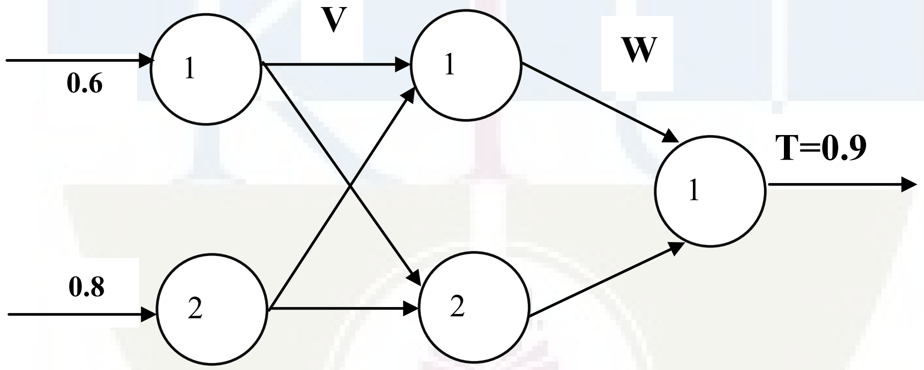
OR

12. (a) With an example classification problem, explain the following terms:
a) Hyper parameters b) Training set c) Validation sets d) Bias e) Variance **(8)**

(b) Determine the regression equation by finding the regression slope coefficient and the intercept value using the following data. **(6)**

x	55	60	65	70	80
y	52	54	56	58	62

13. (a) Update the parameters V_{11} in the given MLP using back propagation with learning rate as 0.5 and activation function as sigmoid. Initial weights are given as V_{11}= 0.2, V_{12}=0.1, V_{21}=0.1, V_{22}=0.3, V_{11}=0.2, W_{11}=0.5, W_{21}=0.2 **(10)**

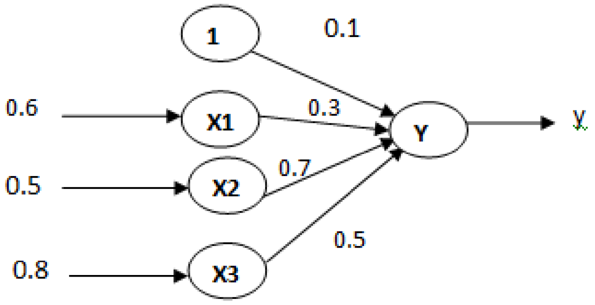


(b) Explain the importance of choosing the right step size in neural networks **(4)**

OR

14. (a) Explain in detail any four practical issues in neural network training **(8)**

(b) Calculate the output of the following neuron Y with the activation function as a) binary sigmoid b) tanh c)ReLU **(6)**



15. (a) Explain, what might happen in ADAGRAD, where momentum is expressed as $\Delta \square_{\square} = -\square\square_{\square}/\sqrt{}(\sum_{\square=1}^{\square} \square_{\square}^{2})$ where the denominator computes the L2 norm of all previous gradients on a per-dimension basis and □ is a global learning rate shared by all dimensions. **(6)**

(b) Differentiate gradient descent with and without momentum. Give equations for weight updation in GD with and without momentum. Illustrate plateaus, saddle points and slowly varying gradients. **(8)**

OR

16. (a) Suppose a supervised learning problem is given to model a deep feed forward neural network. Suggest solutions for the following a) small sized dataset for training b) dataset with both labelled and unlabeled data c) large data set but data from different distribution **(9)**

(b) Describe the effect in bias and variance when a neural network is modified with more number of hidden units followed with dropout regularization. **(5)**

17. (a) Draw and explain the architecture of Convolutional Neural Networks **(8)**

(b) Suppose that a CNN was trained to classify images into different categories. It performed well on a validation set that was taken from the same source as the training set but not on a testing set. What could be the problem with the training of such a CNN? How will you ascertain the problem? How can those problems be solved? **(6)**

OR

18. (a) Explain the following convolution functions a)tensors b) kernel flipping c) down sampling d) strides e) zero padding. **(10)**

(b) What is the motivation behind convolution neural networks? **(4)**

19. (a) Describe how an LSTM takes care of the vanishing gradient problem. Use some hypothetical numbers for input and output signals to explain the concept **(8)**

(b) Explain the architecture of Recurrent Neural Networks **(6)**

OR

20. (a) Explain LSTM based solution for anyone of the problems in the Natural Language Processing domain. **(8)**

(b) Discuss the architecture of GRU **(6)**

Teaching Plan

Module 1 : [Text book 1: Chapter 5, Textbook 2: Chapter 2](9 hours)		
1.1	Introduction, Learning algorithms - Supervised, Unsupervised, Reinforcement	1 hour
1.2	Overfitting, Underfitting, Hyperparameters	1 hour
1.3	Validation sets, Estimators -Bias and Variance. Challenges in machine learning.	1 hour
1.4	Simple Linear Regression	1 hour
1.5	Illustration of Linear Regression	1 hour
1.6	Logistic Regression	1 hour
1.7	Illustration of Logistic Regression	1 hour
1.8	Performance measures - Confusion matrix, Accuracy, Precision, Recall, Sensitivity, Specificity, ROC, AUC.	1 hour
1.9	Illustrative Examples for performance measures	1 hour
Module 2 : Text book 2, Chapter 1 (8 hours)		
2.1	Introduction to neural networks -Single layer perceptrons	1 hour
2.2	Multi Layer Perceptrons (MLPs), Representation Power of MLPs	1 hour
2.3	Activation functions - Sigmoid, Tanh, ReLU, Softmax. Risk minimization, Loss function	1 hour

2.4	Training MLPs with backpropagation	1 hour
2.5	Illustration of back propagation algorithm	1 hour
2.6	Practical issues in neural network training - The Problem of Overfitting, Vanishing and exploding gradient problems	1 hour
2.7	Difficulties in convergence, Local and spurious Optima, Computational Challenges.	1 hour
2.8	Applications of neural networks	1 hour
Module 3 : Text book 1: Chapter 7, 8, Text book 2, Chapter 3, 4 (10 hours)		
3.1	Introduction to deep learning, Deep feed forward network	1 hour
3.2	Training deep models - Introduction, setup and initialization issues	1 hour
3.3	Solving vanishing and exploding gradient problems	1 hour
3.4	Concepts of optimization, Gradient Descent (GD), GD with momentum.	1 hour
3.5	Nesterov accelerated GD, Stochastic GD.	1 hour
3.6	AdaGrad, RMSProp, Adam.	1 hour
3.7	Concepts of Regularization, L1 and L2 regularization.	1 hour
3.8	Early stopping, Dataset augmentation	1 hour
3.9	Parameter sharing and tying, Injecting noise at input, Ensemble methods	1 hour
3.10	Dropout, Parameter initialization.	1 hour
Module 4 : Text book 1, Chapter 9, Text book 2: Chapter 8 (8 hours)		
4.1	Convolutional Neural Networks, architecture	1 hour
4.2	Convolution and Pooling operation with example	1 hour
4.3	Convolution and Pooling as an infinitely strong prior	1 hour
4.4	Variants of convolution functions, structured outputs, data types	1 hour
4.5	Efficient convolution algorithms.	1 hour
4.6	Practical use cases for CNNs	1 hour
4.7	Case study - Building CNN with MNIST and AlexNet.	1 hour
4.8	Case study - Building CNN with MNIST and AlexNet	1 hour
Module 5 : Text book 1 :Chapter 10, 11, Text book 2:Chapter 7 (10 hours)		

5.1	Recurrent neural networks – Computational graphs, RNN design	1 hour
5.2	Encoder – decoder sequence to sequence architectures	1 hour
5.3	Deep recurrent networks- Architecture	1 hour
5.4	Recursive neural networks	1 hour
5.5	Modern RNNs - LSTM	1 hour
5.6	Modern RNNs - LSTM	1 hour
5.7	GRU	1 hour
5.8	Practical use cases for RNNs.	1 hour
5.9	Case study - Natural Language Processing.	1 hour
5.10	Case study - Natural Language Processing.	1 hour

CST 396	ADVANCED TOPICS IN MACHINE LEARNING	Category	L	T	P	Credit	Year of Introduction
		VAC	3	1	0	4	2019

Preamble:

This course enables the learners to understand the advanced concepts and algorithms in machine learning. The course covers the standard and most popular supervised learning algorithms such as linear regression, logistic regression, decision trees, Bayesian learning and the naive Bayes algorithm, basic clustering algorithms, auto encoders, sampling methods and PAC learning. This course helps the students to provide machine learning based solutions to real world problems.

Prerequisite: Basic understanding of probability theory, linear algebra, multivariate calculus and multivariate probability theory.

CO1	Illustrate the concepts of regression and classification techniques **(Cognitive Knowledge Level: Apply)**
CO2	Demonstrate various unsupervised learning techniques **(Cognitive Knowledge Level: Apply)**
CO3	Choose suitable model parameters for different machine learning techniques and to evaluate a model performance **(Cognitive Knowledge Level: Apply)**
CO4	Explain the framework of PAC learning, basic concepts of VC dimension and non-uniform learnability **(Cognitive Knowledge Level: Understand)**
CO5	Construct Bayesian models for data and apply computational techniques to draw inferences **(Cognitive Knowledge Level: Apply)**
CO6	Illustrate the concepts of sampling algorithms, auto encoder, generative adversarial networks **(Cognitive Knowledge Level: Apply)**

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✓	✓	✓	✓	✓	✓						✓
CO2	✓	✓	✓	✓	✓	✓						✓
CO3	✓	✓	✓	✓	✓	✓						✓
CO4	✓	✓	✓	✓								✓
CO5	✓	✓	✓	✓	✓							✓
CO6	✓	✓	✓	✓	✓	✓						✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		End Semester Examination Marks
	Test1 (Percentage)	Test2 (Percentage)	
Remember	**30**	**30**	**30**
Understand	**30**	**30**	**30**
Apply	**40**	**40**	**40**
Analyse			
Evaluate			
Create			

Mark Distribution

Total Marks	CIE Marks	ESE Marks	ESE Duration
150	**50**	**100**	**3 hours**

Continuous Internal Evaluation Pattern:

Attendance : 10 marks

Continuous Assessment Tests : 25 marks

Continuous Assessment Assignment : 15 marks

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks

First Internal Examination shall be preferably conducted after completing the first half of the syllabus and the Second Internal Examination shall be preferably conducted after completing remaining part of the syllabus.

There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly covered module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly covered module), each with 7 marks. Out of the 7 questions in Part B, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which a student should answer any one. Each question can have a maximum 2 sub-divisions and carry 14 marks.

Syllabus

Module -1 (Supervised Learning)

Overview of machine learning - supervised, semi-supervised, unsupervised learning, reinforcement learning Regression algorithms: least squares linear regression, gradient descent, closed form, normal equations, regularization techniques (LASSO, RIDGE), polynomial regression. Discriminative Methods - Logistic Regression, Decision Tree Learning. Generative Methods - Naive Bayes Classifier, Gaussian Discriminant Analysis (GDA).

Module -2 (Unsupervised Learning)

Clustering - Similarity measures, Hierarchical Agglomerative Clustering, K-means partitional clustering, K-medoids clustering, Gaussian mixture models: Expectation Maximization (EM) algorithm for Gaussian mixture model.

Module -3 (Practical aspects in machine learning)

Classification Performance measures - Precision, Recall, Accuracy, F-Measure, ROC, AUC, generalisation and overfitting, cross-validation, bias-variance tradeoff, error estimation, parameter and model selection. Ensemble Methods - Bagging, Boosting, Adaboost, Random Forests.

Module -4 (Statistical Learning Theory)

Models of learnability- learning in the limit, probably approximately correct (PAC) learning. Sample complexity- quantifying the number of examples needed to PAC learn, Computational complexity of training, Sample complexity for finite hypothesis spaces, PAC results for learning conjunctions, Sample complexity for infinite hypothesis spaces, Vapnik-Chervonenkis(VC) dimension.

Module -5 (Advanced Machine Learning Topics)

Graphical models - Bayesian belief networks, Markov random fields(MRFs), Inference on chains and factor graphs, inference on clique trees. Monte Carlo methods – Basic sampling algorithms, rejection sampling, importance sampling, Markov chain Monte Carlo(MCMC), Gibbs sampling. Variational methods. Auto Encoder, Variational AutoEncoder, Generative Adversarial Networks

Textbook

1. Christopher M. Bishop. Pattern recognition and machine learning. Springer 2006.
2. Ethem Alpaydin, Introduction to Machine Learning, 2nd edition, MIT Press 2010.
3. Mohammed J. Zaki and Wagner Meira, Data Mining and Analysis: Fundamental Concepts and Algorithms, Cambridge University Press, First South Asia edition, 2016.
4. Ian Goodfellow, Yoshua Bengio and Aaron Courville. Deep Learning. MIT Press 2016.
5. Mehryar Mohri, Afshin Rostamizadeh and Ameet Talwalkar. Foundations of Machine Learning. Second edition. MIT Press 2018.
6. Tom Mitchell. Machine Learning. McGraw Hill 1997.
7. Richard O. Duda, Peter E . Hart, David G. Stork. Pattern classification, Second Edition. Wiley.
8. Jiawei Han, Micheline Kamber, Jian Pei. Data Mining Concepts and Techniques, Third Edition. Morgan Kaufmann.
9. David Foster. Generative Deep Learning - Teaching Machines to Paint, Write, Compose, and Play. O'Reilly Media, Inc., June 2019.

Reference Books

1. Kevin P. Murphy. Machine Learning: A Probabilistic Perspective. MIT Press 2012
2. Carl Edward Rasmussen and Christopher K. I. Williams. Gaussian Processes for Machine Learning. MIT Press 2005.

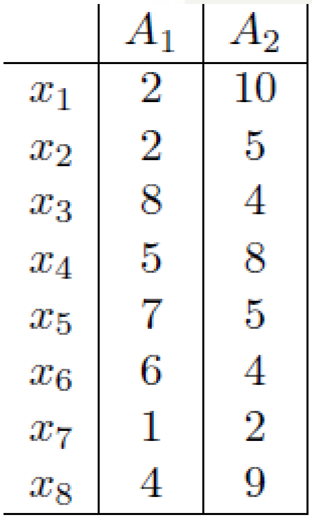
Sample Course Level Assessment Questions

Course Outcome1 (CO1):

1. Consider a naive Bayes classifier with 3 boolean input variables, $\mathbf{X_1}$, $\mathbf{X_2}$ and $\mathbf{X_3}$, and one boolean output, **Y**. How many parameters must be estimated to train such a naive Bayes classifier? How many parameters would have to be estimated to learn the above classifier if we do not make the naive Bayes conditional independence assumption?
2. Describe the ID3 algorithm. Is the order of attributes identical in all branches of the decision tree?
3. Explain the difference between (batch) gradient descent and stochastic gradient descent. Give an example of when you might prefer one over the other.
4. Suppose that you are asked to perform linear regression to learn the function that outputs y, given the D-dimensional input x. You are given N independent data points, and that all the D attributes are linearly independent. Assuming that D is around 100, would you prefer the closed form solution or gradient descent to estimate the regressor?
5. Suppose you have a three class problem where class label y ∈ 0, 1, 2 and each training example X has 3 binary attributes $X_1, X_2, X_3 \in$ **0, 1**. How many parameters (probability distribution) do you need to know to classify an example using the Naive Bayes classifier?

Course Outcome 2(CO2):

1. Which similarity measure could be used to compare feature vectors of two images? Justify your answer.
2. Illustrate the strength and weakness of k-means algorithm.
3. Suppose you want to cluster the eight points shown below using **k**-means



	A_1	A_2
x_1	2	10
x_2	2	5
x_3	8	4
x_4	5	8
x_5	7	5
x_6	6	4
x_7	1	2
x_8	4	9

Assume that **k = 3** and that initially the points are assigned to clusters as follows:

C_1 = {x_1, x_2, x_3}, C_2 = {x_4, x_5, x_6}, C_3 = {x_7, x_8}. Apply the **k**-means algorithm until convergence, using the Manhattan distance.

4. Cluster the following eight points representing locations into three clusters: ***A_1(2, 10), A_2(2, 5), A_3(8, 4), A_4(5, 8), A_5(7, 5), A_6(6, 4), A_7(1, 2), A_8(4, 9)***.

   Initial cluster centers are: ***A_1(2, 10), A_4(5, 8)*** and ***A_7(1, 2)***.

   The distance function between two points ***a = (x_1, y_1)*** and ***b = (x_2, y_2)*** is defined as ***D(a, b)*** = $|x_2 – x_1| + |y_2 – y_1|$

   Use **k**-Means Algorithm to find the three cluster centers after the second iteration.

Course Outcome 3(CO3):

1. What is ensemble learning? Can ensemble learning using linear classifiers learn classification of linearly non-separable sets?
2. Describe boosting. What is the relation between boosting and ensemble learning?
3. Classifier A attains 100% accuracy on the training set and 70% accuracy on the test set. Classifier B attains 70% accuracy on the training set and 75% accuracy on the test set. Which one is a better classifier. Justify your answer.
4. What are ROC space and ROC curve in machine learning? In ROC space, which points correspond to perfect prediction, always positive prediction and always negative prediction? Why?
5. Suppose there are three classifiers A,B and C. The (FPR, TPR) measures of the three classifiers are as follows – A (0, 1), B (1, 1) , C (1,0.5). Which can be considered as a perfect classifier? Justify your answer.

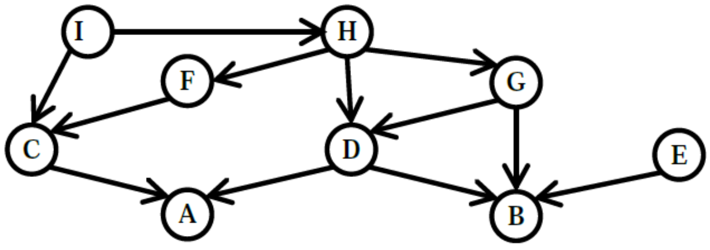
Course Outcome 4(CO4): .

1. A monotone conjunction is a conjunction of the variables such that no variable is negated. Show that the concept class of monotone conjunction is probably approximately correct (PAC)-learnable.
2. Consider a Boolean classification problem with ***n*** binary variables and a hypothesis space ***H***, where each hypothesis is a decision tree of depth 2, using only two variables. How many training examples, ***m*** suffice to assure that with probability at least 0.99, any consistent learner using ***H*** will output a hypothesis with true error at most 0.05
3. Show that the concept class C containing the set of all boolean functions on n variable is not PAC-learnable.

4. What is the Vapnik-Chervonenkis(VC)-dimension of a circle centered at the origin.
5. A hypothesis space that has a high VC dimension is good, bad, or neither? Explain in terms of both (a) richness or expressive power of the hypotheses, and (b) sample complexity.

Course Outcome 5(CO5):

1. Write down the factored conditional probability expression that corresponds to the graphical Bayesian Network shown below.



2. How do we learn the conditional probability tables(CPT) in Bayesian networks if information about some variables is missing? How are these variables called?

Course Outcome 6 (CO6):

1. Derive an algorithm using the inverse transform method to generate a random sample from the exponential distribution.
2. Explain the pros and cons of importance sampling versus rejection sampling.
3. Sketch the core idea of the Monte Carlo method. What is a sample? What is a direct sampling method? Why can't it be used directly to do any inference? What is rejection sampling? What is its major disadvantage?
4. Generative Adversarial Networks(GANs) include a generator and a discriminator. Sketch a basic GAN using those elements, a source of real images, and a source of randomness.
5. The word "adversarial" in the acronym for GANs suggests a two-player game. What are the two players, and what are their respective goals?

Model Question Paper

QP CODE:

Reg No: _______________

Name: _________________ **PAGES : 5**

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SIXTH SEMESTER B.TECH DEGREE EXAMINATION (HONORS), MONTH & YEAR

Course Code: CST 396

Course Name: Advanced Topics in Machine Learning

Max.Marks:100 **Duration: 3 Hours**

PART A

Answer All Questions. Each Question Carries 3 Marks

1.	Suppose you have a dataset with m = 1000000 examples and n = 200000 features for each example. You want to use multivariate linear regression to fit the parameters to our data. Should you prefer gradient descent or the normal equation? Justify your answer.	
2.	Define Information gain? How is that different from Gain ratio? Give the advantage of using Gain ratio measure?	
3.	What is cluster analysis? Identify two applications where cluster analysis can be applied to multimedia data?	
4.	Given two objects represented by the tuples (22, 1, 42, 10) and (20, 0, 36, 8): (i) Compute the Euclidean distance between the two objects. (ii) Compute the Manhattan distance between the two objects.	
5.	Suppose there are three classifiers A,B and C. The (FPR, TPR) measures of the three classifiers are as follows – A (0, 1), B (1, 1) , C (1,0.5). Which can be considered as a perfect classifier? Justify your answer.	
6.	How Bias-Variance Tradeoff affects machine learning algorithms?	
7.	For a particular learning task, if the requirement of error parameter ε changes from 0.1 to 0.01. How many more samples will be required for probably approximately correct(PAC) learning?	

8. Suppose we have a hypothesis set that labels all points inside an interval ***[a, b]*** as class 1. Find its Vapnik-Chervonenkis(VC)- dimension?

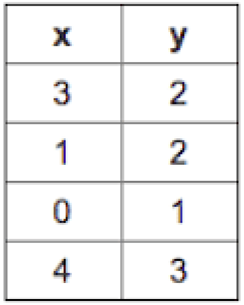
9. Given a density function ***f(x)***, the rejection sampling is a method that can generate data points from the density function ***f***. List the three steps to generate a random sample from f using rejection sampling.

10. How does the variational auto-encoder(VAE) architecture allow it to generate new data points, compared to auto-encoder, which cannot generate new data points? **(10x3=30)**

Part B

(Answer any one question from each module. Each question carries 14 Marks)

11. (a) Consider the hypothesis for the linear regression $h_\theta (x) = \theta_0 + \theta_1 x$, and the cost function $J(\theta_0, \theta_1) = 1/2m \Sigma_{i= 1} \text{ to } m (h_\theta (x^{(i)}) - y^{(i)})^2$ where m is the number of training examples. Given the following set of training examples. **(5)**



x	y
3	2
1	2
0	1
4	3

Answer the following questions :

1) Find the value of $h_\theta (2)$ if $\theta_0 = 0$ and $\theta_1 = 1.5$

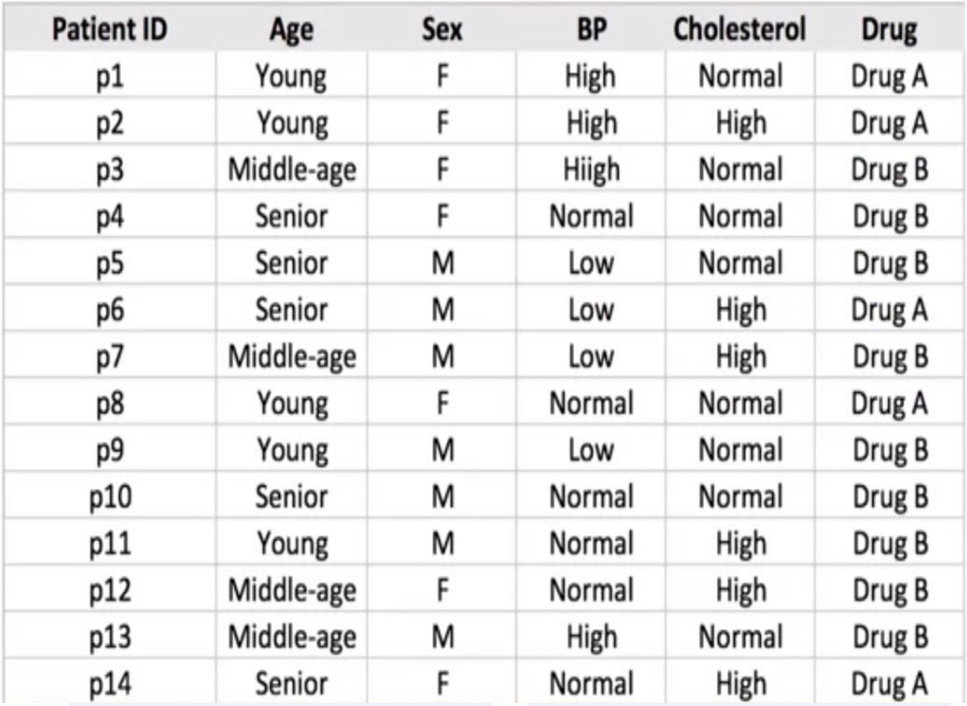
2) Find the value of J(0,1)

3) Suppose the value of $J(\theta_0, \theta_1) = 0$. What can be inferred from this.

(b) Write a gradient descent algorithm for multivariate regression? Compare the gradient and analytical solution to the multivariate regression? **(9)**

OR

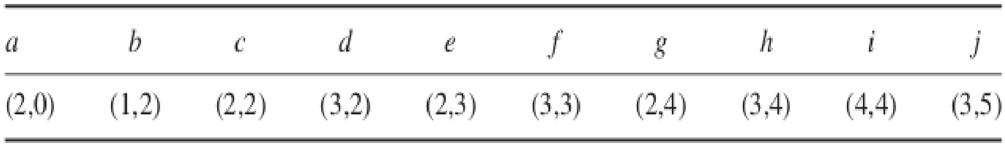
12. (a) Consider the collection of training samples (S) in the Figure given below. Drug is the target attribute which describes the Drug suggested for each patient. Find the value of the following . i) Gain(S, Sex) ii) Gain (S, Cholesterol) **(9)**



Patient ID	Age	Sex	BP	Cholesterol	Drug
p1	Young	F	High	Normal	Drug A
p2	Young	F	High	High	Drug A
p3	Middle-age	F	Hiigh	Normal	Drug B
p4	Senior	F	Normal	Normal	Drug B
p5	Senior	M	Low	Normal	Drug B
p6	Senior	M	Low	High	Drug A
p7	Middle-age	M	Low	High	Drug B
p8	Young	F	Normal	Normal	Drug A
p9	Young	M	Low	Normal	Drug B
p10	Senior	M	Normal	Normal	Drug B
p11	Young	M	Normal	High	Drug B
p12	Middle-age	F	Normal	High	Drug B
p13	Middle-age	M	High	Normal	Drug B
p14	Senior	F	Normal	High	Drug A

(b) Explain how LASSO regression helps to reduce the overfitting problem? **(5)**

13. (a) Suppose that we have the following data: **(9)**



a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*
(2,0)	(1,2)	(2,2)	(3,2)	(2,3)	(3,3)	(2,4)	(3,4)	(4,4)	(3,5)

Identify the cluster by applying the k-means algorithm, with k = 2. Try using initial cluster centers as far apart as possible.

(b) Describe EM algorithm for Gaussian mixtures. **(5)**

OR

14. (a) Illustrate the strength and weakness of k-means in comparison with the k-medoids algorithm. **(4)**

(b) Suppose that we have the following data . Use single linkage Agglomerative clustering to identify the clusters. Draw the Dendogram. Use Euclidean distance measure **(10)**

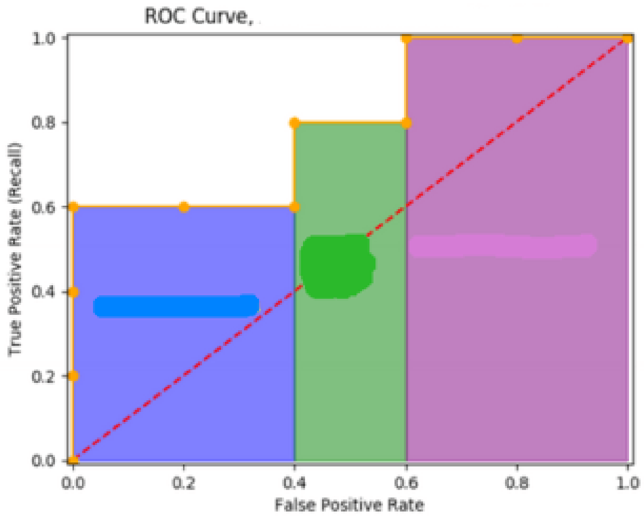
	X	Y
P1	0.4	0.53
P2	0.22	0.38
P3	0.35	0.32
P4	0.26	0.19
P5	0.08	0.41
P6	0.45	0.30

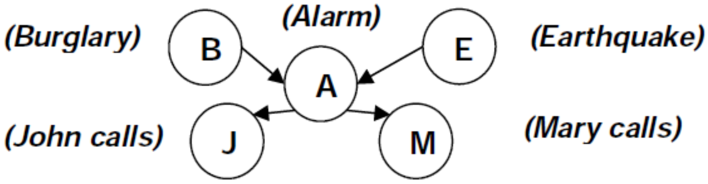
15.	(a)	Define Precision, Recall, Accuracy and F-measure?	**(4)**
	(b)	What does it mean for a classifier to have a high precision but low recall?	**(3)**
	(c)	Fill in the missing values in the accompanying three class confusion matrix. Given that model accuracy is 72% and classification error for class 2 is 20%. Find also the precision and recall for class1	**(7)**

		Predicted		
		Class 1	**Class 2**	**Class 3**
Actual	**Class 1**	14	2	5
	Class 2	?(X)	40	2
	Class 3	1	?(Y)	18

OR

<table>
<tr><td>16.</td><td>(a)</td><td>What are ROC space and ROC curve in machine learning? In ROC space, which points correspond to perfect prediction, always positive prediction and always negative prediction? Why?</td><td><b>(4)</b></td></tr>
<tr><td></td><td>(b)</td><td>Given the following ROC Curve? Find the AUC?


</td><td><b>(3)</b></td></tr>
<tr><td></td><td>(c)</td><td>How does random forest classifier work? Why is a random forest better than a decision tree?</td><td><b>(7)</b></td></tr>
<tr><td>17.</td><td>(a)</td><td>Show that the concept class Cn of the conjunction of boolean literals up to n variables is probably approximately correct(PAC)-learnable.</td><td><b>(8)</b></td></tr>
<tr><td></td><td>(b)</td><td>Explain the concept of Vapnik-Chervonenkis (VC) dimension using shattering. How the number of training examples required to train the model is related to the VC dimension and what is its relation with training and test errors.</td><td><b>(6)</b></td></tr>
<tr><td colspan="4"><b>OR</b></td></tr>
<tr><td>18.</td><td>(a)</td><td>Consider a Boolean classification problem with <b><i>n</i></b> binary variables and a hypothesis space <b><i>H</i></b>, where each hypothesis is a decision tree of depth 1. How many training examples, <b><i>m</i></b> suffice to assure that with probability at least 0.99, any consistent learner using <b><i>H</i></b> will output a hypothesis with true error at most 0.05?</td><td><b>(7)</b></td></tr>
<tr><td></td><td>(b)</td><td>Prove that VC(H) ≤ log2 |H|, where H is a hypothesis space. (|H| denotes the</td><td><b>(7)</b></td></tr>
</table>

<table>
<tr><td></td><td></td><td>cardinality of the hypothesis space)</td><td></td></tr>
<tr><td>19.</td><td>(a)</td><td>Shown below is the Bayesian network corresponding to the Burglar Alarm problem, P(J | A) P(M | A) P(A | B, E) P(B) P(E). The probability tables show the probability that variable is True, e.g., P(M) means P(M = t). Find P(J = t ∧ M = f ∧ A = f ∧ B = f ∧ E = t).


<table><tr><th>P(E)</th></tr><tr><td>.002</td></tr></table>
<table><tr><th>A</th><th>P(M)</th></tr><tr><td>t</td><td>.70</td></tr><tr><td>f</td><td>.01</td></tr></table>
<table><tr><th>B</th><th>E</th><th>P(A)</th></tr><tr><td>t</td><td>t</td><td>.95</td></tr><tr><td>t</td><td>f</td><td>.94</td></tr><tr><td>f</td><td>t</td><td>.29</td></tr><tr><td>f</td><td>f</td><td>.001</td></tr></table>
<table><tr><th>A</th><th>P(J)</th></tr><tr><td>t</td><td>.90</td></tr><tr><td>f</td><td>.05</td></tr></table>
<table><tr><th>P(B)</th></tr><tr><td>.001</td></tr></table>
</td><td><b>(7)</b></td></tr>
<tr><td></td><td>(b)</td><td>Derive an algorithm using the inverse transform method to generate a random sample from the distribution with density $f_X(x) = 3\,x^2,\ 0 < x < 1$.</td><td><b>(7)</b></td></tr>
<tr><td colspan="4"><b>OR</b></td></tr>
<tr><td>20.</td><td>(a)</td><td>Draw the Bayesian Network that corresponds to this conditional probability: <b><i>P(A | B,C,E) P(B | D,E) P(C | F,H) P(D | G) P(E| G,H) P(F | H) P(G) P(H)</i></b></td><td><b>(6)</b></td></tr>
<tr><td></td><td>(b)</td><td>What is effective sample size (ESS)? Why is a large ESS necessary but not sufficient for good MCMC mixing?</td><td><b>(3)</b></td></tr>
<tr><td></td><td>(c)</td><td>Describe the overall Gibbs sampling algorithm briefly</td><td><b>(5)</b></td></tr>
</table>

Teaching Plan

Module 1 : (Supervised Learning)(10 hours)		
1.1	Supervised, semi-supervised, unsupervised learning, reinforcement learning (TB 2: Ch 1)	1 hour
1.2	Least squares linear regression (TB 2: Section 2.6)	1 hour
1.3	Gradient descent, closed form, normal equations (TB 2: Section 5.8)	1 hour
1.4	Regularization techniques (LASSO, RIDGE) (TB 4: Section 7.1)	1 hour
1.5	Polynomial regression (TB 2: Section 2.6)	1 hour
1.6	Logistic Regression (TB 6: Section 3.3)	1 hour
1.7	Decision Tree Learning (ID3) (TB 8: Section 8.2)	1 hour
1.8	Decision Tree Learning (C4.5) (TB 8: Section 8.2)	1 hour
1.9	Naive Bayes Classifier (TB 8: Section 8.3)	1 hour
1.10	Gaussian Discriminant Analysis (GDA) (TB 7: Section 5.2,5.3)	1 hour
Module 2 : (Unsupervised Learning)(8 hours)		
2.1	Similarity measures (TB 8: Section 2.4)	1 hour
2.2	Hierarchical Agglomerative Clustering (TB 3: Chapter 14)	1 hour
2.3	Hierarchical Agglomerative Clustering (TB 3: Chapter 14)	
2.4	K-means partitional clustering (TB 3: Chapter 13)	1 hour
2.5	K-medoids partitional clustering	
2.6	Gaussian mixture models (TB 3: Chapter 13)	1 hour
2.7	Expectation Maximization (EM) algorithm for Gaussian mixture model Lecture-1 (TB 3: Chapter 13)	1 hour
2.8	Expectation Maximization (EM) algorithm for Gaussian mixture model Lecture-2 (TB 3: Chapter 13)	1 hour
Module 3 : (Practical aspects in machine learning) (6 hours)		

3.1	Precision, Recall, Accuracy, F-Measure, ROC, AUC (TB8.5/TB 3: Chapter 22.1)	1 hour
3.2	Generalisation and overfitting, cross-validation (TB 2: Section 2.7,4.8)	1 hour
3.3	Bias-variance tradeoff (TB 2: Chapter 22.3)	1 hour
3.4	Error estimation, parameter and model selection (TB 3: Chapter 8.5)	1 hour
3.5	Bagging, Boosting (TB 8: Chapter 8.6)	1 hour
3.6	Adaboost, Random Forests (TB 8: Chapter 8.6)	1 hour
Module 4 : (Statistical Learning Theory) (TB 5 – Chapter 2, 3.3)(7 hours)		
4.1	Learning in the limit, probably approximately correct (PAC) learning	1 hour
4.2	Quantifying the number of examples needed to PAC learn	1 hour
4.3	Computational complexity of training	1 hour
4.4	Sample complexity for finite hypothesis spaces	1 hour
4.5	PAC results for learning conjunctions	1 hour
4.6	Sample complexity for infinite hypothesis spaces	1 hour
4.7	Vapnik-Chervonenkis(VC) dimension	1 hour
Module 5 : (Advanced Machine Learning Topics) (13 hours)		
5.1	Bayesian belief networks (TB 1 – Chapter 8)	1 hour
5.2	Markov random fields (TB 1 – Chapter 8)	1 hour
5.3	Inference on chains and factor graphs (TB 1 – Chapter 8)	1 hour
5.4	Inference on clique trees (TB 1 – Chapter 8)	1 hour
5.5	Basic sampling algorithms (TB 1 – Chapter 11)	1 hour
5.6	Rejection sampling (TB 1 – Chapter 11)	1 hour
5.7	Importance sampling (TB 1 – Chapter 11)	1 hour
5.8	Markov chain Monte Carlo(MCMC) (TB 1 – Chapter 11)	1 hour
5.9	Gibbs sampling (TB 1 – Chapter 11)	1 hour

5.10	Variational method (TB 1 – Chapter 10)	1 hour
5.11	Auto Encoder (TB 4 – Chapter 14)	1 hour
5.12	Variational AutoEncoder (TB 9 – Chapter 3)	1 hour
5.13	Generative Adversarial Networks (TB 9 – Chapter 4)	1 hour

CST 397	**PRINCIPLES OF MODEL CHECKING**	**Category**	**L**	**T**	**P**	**Credit**	**Year of Introduction**
		VAC	**3**	**1**	**0**	**4**	**2019**

Preamble:
This course covers the basic theory and algorithm for an automatic verification process namely, model checking. Model checking is a formal process for proving the correctness of a hardware/software which can be modelled as a finite-state transition system. This course introduces the topics - finite-state modelling of hardware/software, linear-time properties, classification of linear-time properties, Linear Temporal Logic (LTL), a formal language for property specification, LTL model checking algorithm and model checking case studies. Proving correctness of a hardware/software is essential in safety critical systems in domains such as avionics, health care and automotive.

Prerequisite: Nil

Course Outcomes: After the completion of the course, the student will be able to

CO#	**Course Outcomes**
CO1	Illustrate an application for model checking. **(Cognitive Knowledge Level: Understand)**
CO2	Describe finite-state modelling of hardware and software. **(Cognitive Knowledge Level: Understand)**
CO3	Identify the linear-time properties required to represent the requirements of a system. **(Cognitive Knowledge Level: Apply**)
CO4	Specify a given linear-time property in Linear Temporal Logic (LTL). (**Cognitive Knowledge Level: Apply**)
CO5	Perform LTL model checking with the tool SAL (Symbolic Analysis Laboratory). (**Cognitive Knowledge Level: Apply**)

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✓	✓	✓	✓	✓	✓						✓
CO2	✓	✓	✓	✓								✓
CO3	✓	✓	✓	✓								✓
CO4	✓	✓	✓	✓								✓
CO5	✓	✓	✓	✓								✓
CO6	✓	✓	✓	✓	✓	✓						✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	**Test 1 (Marks in percentage)**	**Test 2 (Marks in percentage)**	**End Semester Examination (Marks in percentage)**
Remember	30	30	30
Understand	40	40	40
Apply	40	40	40
Analyze			
Evaluate			
Create			

Mark Distribution

Total Marks	**CIE Marks**	**ESE Marks**	**ESE Duration**
150	**50**	**100**	**3**

Continuous Internal Evaluation Pattern:

Attendance	: **10 marks**
Continuous Assessment Test	: **25 marks**
Continuous Assessment Assignment	: **15 marks**

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks. The first series test shall be preferably conducted after completing the first half of the syllabus. The second series test shall be preferably conducted after completing the remaining part of the syllabus. There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly completed module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly completed module), each with 7 marks. Out of the 7 questions, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which a student should answer anyone. Each question can have maximum 2 sub-divisions and carries 14 marks.

Syllabus

Module 1 (Introduction to Model Checking)

System Verification– Hardware and Software Verification, Model Checking, Characteristics of Model Checking. Transition Systems – Transition System, Direct Predecessors and Successors, Terminal State, Deterministic Transition System.
Executions - Execution Fragment, Maximal and Initial Execution Fragment, Execution, Reachable States. Modeling Hardware and Software Systems- Sequential Hardware Circuits, data Dependent Systems.

Module - 2 (Linear Time Properties)

Linear-Time (LT) Properties - Deadlock. Linear-Time Behavior - Paths and State Graph, Path Fragment, Maximal and Initial Path Fragment, Path. Traces - Trace and Trace Fragment, LT Properties - LT Property, Satisfaction Relation for LT Properties, Trace Equivalence and LT Properties. Safety Properties and Invariants - Invariants, Safety Properties, Trace Equivalence and Safety properties. Liveness Properties - Liveness Property, Safety vs. Liveness Properties. Fairness - Fairness, Unconditional, Weak and Strong Fairness, Fairness Strategies, Fairness and Safety. (Definition and examples only for all topics - no proof required).

Module - 3 (Regular Properties)

Regular Properties - Model Checking Regular Safety properties - Regular Safety property, Verifying Regular Safety Properties. Automata on Infinite Words - ω-Regular Languages and Properties, Nondeterministic Buchi Automata (NBA), Deterministic Buchi Automata (DBA), Generalised Buchi Automata (Definitions only). Model Checking ω-Regular Properties - Persistence Properties and Product, Nested Depth-First Search (Only algorithms required).

Module - 4 (Linear Time Logic)

Linear Temporal Logic (LTL) - Syntax, Semantics, Equivalence of LTL Formulae, Weak Until, Release and Positive Normal Form, Fairness, Safety and Liveness in LTL (Definitions only). Automata Based LTL Model Checking (Algorithms and examples only).

Module - 5 (Model Checking in SAL)

Introduction - Introduction to the tool Symbolic Analysis Laboratory (SAL). The Language of SAL - The expression language, The transition Language, The module language, SAL Contexts. SAL Examples - Mutual Exclusion, Peterson's Protocol, Synchronous Bus Arbiter, Bounded Bakery protocol, Bakery Protocol, Simpson's Protocol, Stack.

Text Books

1. Christel Baier and Joost-Pieter Katoen, Principles of Model Checking, The MIT Press. (Modules 1 - 4)
2. Leonardo de Moura, Sam Owre and N. Shankar, The SAL Language Manual, SRI International (http://sal.csl.sri.com/doc/language-report.pdf, Chapters 1, 3, 4, 5, 6, 7) (Module 5)

Reference Materials

1. SAL Examples (http://sal.csl.sri.com/examples.shtml) (Module 5)

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Explain how model checking can be effective in developing a nuclear power plant.

Course Outcome 2 (CO2):

1. Consider a message delivery system. The sender *s* is trying to send a series of messages to the receiver *r* in such a way that the $(i+1)^{st}$ message is sent only after the i^{th} message is delivered. There is a possibility of error in sending a message and in that case, *s* keeps on trying until it is able to send the message. Express this process as a transition system.

Course Outcome 3 (CO3):

1. Consider a shared memory segment *s* protected using a mutex lock variable *m*. Two processes p_1 and p_2 are trying to access *s*. Find the Linear Time properties of the system which will ensure safety, liveness and fairness.

Course Outcome 4 (CO4):

1. Express the Linear Time properties found in the above system using LTL.

Course Outcome 5 (CO5):

1. Model the above system using SAL and verify that the system avoids deadlock under all conditions.
2.

Model Question Paper

QP CODE: **PAGES: ___**

Reg No:_______________

Name:__________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIFTH SEMESTER B.TECH DEGREE EXAMINATION(HONORS), MONTH & YEAR

Course Code: CST 397

Course Name : Principles of Model Checking

Max Marks: 100 **Duration: 3 Hours**

PART-A

(Answer All Questions. Each question carries 3 marks)

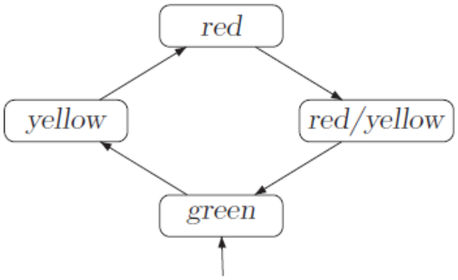
1. What is model checking? Give the schematic view of the model checking approach.

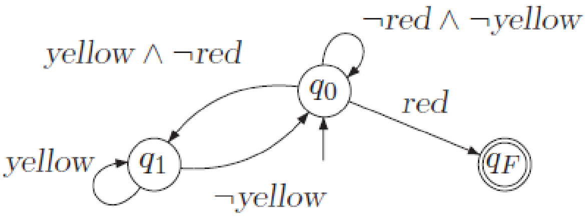
2. Give the transition system of a beverage vending machine.

3. What is an invariant in Linear Time (LT) properties? Give an example.

4. Give 3 Liveness properties in the Mutual Exclusion problem of processes.

5. Find the product automaton for the following Transition System and Non-Deterministic Finite Automaton (NFA).





6. Differentiate between Deterministic Buchi Automaton and Non-deterministic

Buchi Automaton. Give examples of each.

7. Express the following statements about traffic lights in Linear Temporal Logic (LTL).
   a. Once red, the light can not become green immediately.
   b. Once red, the light always becomes green eventually after being yellow for some time.

8. What is Positive Normal Form (PNF) in LTL? Give an example.

9. Write notes on Symbolic Analysis Laboratory (SAL).

10. What is a SAL context? Give an example.

(10x3=30)

Part B

(Answer any one question from each module. Each question carries 14 Marks)

11. (a) Explain in detail the various phases of the model checking process. **(7)**

    (b) Explain the strengths and weaknesses of model checking. **(7)**

OR

12. (a) Explain the following terms in association with execution of a transition system. **(14)**
    a. Execution Fragment
    b. Maximal and Initial Execution Fragment
    c. Execution
    d. Reachable States

13. (a) With an example, explain the satisfaction relation for LT properties. **(7)**

    (b) What is trace equivalence in Transition Systems? Give an example to show that if two transition systems have the same trace equivalence, they satisfy the same LT properties. **(7)**

14. (a) Give the transition system for the fault tolerant variant of the dining philosophers problem. **(4)**

(b) With a suitable example, explain the algorithms to check whether a Transition System satisfies an invariant or not. **(10)**

15. (a) Give the algorithm for verifying Regular Safety Properties. Explain with an appropriate example. **(7)**

(b) With a suitable example, explain Regular Safety Properties. **(7)**

OR

16. (a) Explain ω -Regular Properties. **(4)**

(b) Illustrate how ω -Regular Properties are verified. **(10)**

17. (a) Explain the syntax of Linear Temporal Logic (LTL). **(7)**

(b) Explain the semantics of LTL. **(7)**

OR

18. (a) With an example, give the difference between *until* and *weak until* in LTL. **(4)**

(b) With a suitable example, explain automata based LTL model checking. **(10)**

19. (a) Explain Peterson's protocol. What are the LTL properties to be verified to ensure its correctness? **(8)**

(b) Write a SAL script for the verification of Peterson's protocol. **(6)**

OR

20. (a) Show the SAL model corresponding to Bakery protocol. **(8)**

(b) List any three Linear Time properties of this model and show their LTL specifications. **(6)**

Teaching plan

	Module 1 (Introduction to Model Checking)	**8 Hours**
1.1	**System Verification** – Hard- and Software Verification, Model Checking, Characteristics of Model Checking	1 Hour
1.2	Transition Systems – Transition System, Direct Predecessors and Successors,	1 Hour
1.3	Terminal State, Deterministic Transition System,	1 Hour
1.4	**Executions** - Execution Fragment, Maximal and Initial Execution Fragment	1 Hour
1.5	Execution, Reachable States	1 Hour
1.6	Modeling Hardware and Software Systems - Sequential Hardware Circuits	1 Hours
1.7	Data Dependent Systems (Lecture 1)	1 Hour
1.8	Data Dependent Systems (Lecture 2)	1 Hour
	Module 2 (Linear Time Properties)	**10 Hours**
2.1	Linear-Time (LT) Properties - Deadlock	1 Hour
2.2	Linear-Time Behavior - Paths and State Graph, Path Fragment	1 Hour
2.3	Maximal and Initial Path Fragment, Path	
2.4	Traces - Trace and Trace Fragment	1 Hour
2.5	LT Property, Satisfaction Relation for LT Properties, Trace Equivalence and LT Properties	1 Hour
2.6	Invariants	1 Hour
2.7	Safety Properties, Trace Equivalence and Safety properties	1 Hour
2.8	Liveness Property, Safety vs. Liveness Properties	1 Hour
2.9	Fairness, Unconditional, Weak and Strong Fairness	1 Hour
2.10	Fairness Strategies, Fairness and Safety	1 Hour
	Module 3 (Regular Properties)	**8 Hours**
3.1	**Regular Properties** - Model Checking Regular Safety properties - Regular Safety property	1 Hour
3.2	Verifying Regular Safety Properties	1 Hour

3.3	Automata on Infinite Words - ω-Regular Languages and Properties	1 Hour
3.4	Nondeterministic Buchi Automata (NBA), Deterministic Buchi Automata (DBA), Generalised Buchi Automata	1 Hour
3.5	Model Checking ω-Regular Properties - Persistence Properties and Product - Lecture 1	1 Hour
3.6	Persistence Properties and Product - Lecture 2	1 Hour
3.7	Nested Depth-First Search (Lecture 1)	1 Hour
3.8	Nested Depth-First Search (Lecture 2)	1 Hour
Module 4 (Linear Time Logic)		**9 Hours**
4.1	Linear Temporal Logic – Linear Temporal Logic (LTL) - Syntax	1 Hour
4.2	Semantics - Lecture 1	1 Hour
4.3	Semantics - Lecture 2	1 Hour
4.4	Equivalence of LTL Formulae, Weak Until	1 Hour
4.5	Release and Positive Normal Form	1 Hour
4.6	Fairness, Safety and Liveness in LTL	1 Hour
4.7	Automata Based LTL Model Checking - Lecture 1	1 Hour
4.8	Automata Based LTL Model Checking - Lecture 2	1 Hour
4.9	Automata Based LTL Model Checking - Lecture 3	1 Hour
Module 5 (Model Checking in SAL)		**10 Hours**
5.1	Introduction - Introduction to the tool Symbolic Analysis Laboratory (SAL).	1 Hour
5.2	The Language of SAL - The expression language, The transition Language	1 Hour
5.3	The module language, SAL Contexts.	1 Hour
5.4	SAL Examples - Mutual Exclusion	1 Hour
5.5	Peterson's Protocol	1 Hour
5.6	Synchronous Bus Arbiter	1 Hour
5.7	Bounded Bakery protocol,	1 Hour
5.8	Bakery Protocol	1 Hour

5.9	Simpson’s Protocol	1 Hour
5.10	Stack	1 Hour

CST 398	THEORY OF COMPUTABILITY AND COMPLEXITY	Category	L	T	P	Credit	Year of Introduction
		VAC	3	1	0	4	2019

Preamble:

This is a theoretical course in computer science to enable the learners to know the fundamentals of computability and complexity theories. It covers the notions of computability/decidability, the process of reduction to prove decidability/undecidability and the classification of problems into class P, class NP and class NP Complete based on the time complexity of solving the problems. This course helps the learner to identify whether a real life problem is decidable/undecidable and also to classify a decidable problem into tractable or intractable, based on the time complexity class it belongs.

Prerequisite: Sound knowledge in Data Structures and Formal Languages and Automata Theory.

Mapping of course outcomes with program outcomes

CO1	Illustrate relative computing powers of Finite State Automata, Push Down Automata, Linear Bounded Automata and Turing Machines.**(Cognitive Knowledge Level: Apply)**
CO2	Prove that a given language is undecidable/not semi-decidable by using the reduction process.**(Cognitive Knowledge Level: Apply)**
CO3	Describe the time complexity of a given problem as a function of the number of steps required by a Turing machine to solve it. **(Cognitive Knowledge Level: Understand)**
CO4	Utilize polynomial time reduction to prove that a given problem is NP Complete. **(Cognitive Knowledge Level: Apply)**

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✓	✓	✓	✓								✓
CO2	✓	✓	✓	✓								✓

CO3	✓	✓	✓	✓								✓
CO4	✓	✓	✓	✓								✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**		**End Semester Examination Marks (%)**
	Test 1 (%)	**Test 2 (%)**	
Remember	**30**	**30**	**30**
Understand	**30**	**30**	**30**
Apply	**40**	**40**	**40**
Analyze			
Evaluate			
Create			

Mark Distribution

Total Marks	CIE Marks	ESE Marks	ESE Duration
150	50	100	3

Continuous Internal Evaluation Pattern:

Attendance	**10 marks**
Continuous Assessment Tests(Average of Internal Tests1&2)	**25 marks**
Continuous Assessment Assignment	**15 marks**

Internal Examination Pattern

Each of the two internal examinations has to be conducted out of 50 marks. First series test shall be preferably conducted after completing the first half of the syllabus and the second series test shall be preferably conducted after completing remaining part of the syllabus. There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly completed module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly completed module), each with 7 marks. Out of the 7 questions, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 full questions from each module of which student should answer any one. Each question can have maximum 2 sub-divisions and carries 14 marks.

Syllabus

Module - 1 (Introduction to Formal Language Theory and Regular Languages)

Finite State Automata, Push Down Automata, Linear Bounded Automata, Turing Machines, Recursive Languages, Recursively Enumerable Languages, Universal Turing Machine, Enumeration Machine, Two Counter Machine.

Module– 2 (Undecidability)

Halting Problem, Language representation of a problem, Reduction - applications, Rice’s First and Second Theorem with proof.

Module - 3 (Overview of Complexity Classes)

Measuring time complexity, Asymptotic notations - Big O and small-o, Analysing algorithms, Complexity relationship among models. Complexity classes- Class P, example problems in class P, Class NP, Polynomial time verification, example problems in class NP.

Module- 4 (NP Completeness)

Satisfiability problem, Polynomial time reducibility, Overview of Graphs, NP Complete Problems, Cook-Levin theorem (SAT is NP Complete).

Module- 5 (More NP Complete Problems)

CLIQUE, Vertex Cover and Hamiltonian path with proof of correctness of NP Completeness.

Text Books

1. Dexter C. Kozen, Automata and Computability, Springer (1999)
2. Michael Sipser, Introduction to the Theory of Computation, Second Edition

Reference Books

1. Douglas B. West, Introduction to Graph Theory, Second Edition

Course Level Assessment Questions

Course Outcome1 (CO1):

Identify the class of the following languages in Chomsky Hierarchy:

1. Design a Finite State Automaton for the language $L = \{axb | x \in \{a, b\}^*\}$
2. Design a Push Down Automaton for the language $L = \{a^n b^n | n \geq 0\}$
3. Design a Linear Bounded Automaton for the language $L = \{a^n b^n c^n | n \geq 0\}$
4. Design a Turing Machine for the language $L = \{ww | w \in \{a, b\}^*\}$

Course Outcome 2(CO2):

Without using Rice's Theorem prove that neither the set FIN (refer Text Book 1) nor its complement is recursively enumerable.

Course Outcome 3(CO3):

Show that the language $L = \{a^n b^n | n \geq 0\}$ can be decided by a deterministic Turing Machine in quadratic time.

Course Outcome 4(CO4): .

Using polynomial time reduction, prove that SUBSET-SUM (refer Text Book 2) problem is NP Complete.

Model Question Paper

QP CODE:

Reg No: _______________

Name: _________________ **PAGES : 4**

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SIXTH SEMESTER B.TECH. DEGREE EXAMINATION(HONORS), MONTH & YEAR

Course Code: CST 398

Course Name: Theory of Computability and Complexity

Max.Marks:100 **Duration: 3 Hours**

PART A

Answer All Questions. Each Question Carries 3 Marks

1. Design a Deterministic Finite state Automaton (DFA) for the language:$L = \{x \in \{0,1\}^* | x does\ not\ contain\ consecutive\ zeros\}$.

2. Design a Pushdown Automaton (PDA) for the language $L = \{a^m b^n | m \geq 0 and n > m\}$ (no explanation is required, just list the transitions in the PDA).

3. List any *six* undecidable problems.

4. Illustrate how a problem can be represented as a language.

5. Describe the term time complexity class.

6. Define the term polynomial time verification. Describe its usage.

7. Define the term polynomial time reduction. Describe its usage.

8. Define vertex cover. Illustrate with the help of a graph.

9. Illustrate CLIQUE problem with an example.

10. State Hamiltonian path problem. Show an example.

(10x3=30)

Part B

(Answer any one question from each module. Each question carries 14 Marks)

11. (a) Why the family of languages recognized by Turing machines is called Recursively Enumerable? Explain the working of an enumeration machine. **(8)**

(b) Illustrate the functioning of a Universal Turing Machine. **(6)**

OR

12. (a) Illustrate the functioning of a two counter machine. **(4)**

(b) Prove that Turing Machines and Two Counter Machines are equivalent in power. **(10)**

13. (a) Prove using Diagonalisation that halting problem is undecidable. **(8)**

(b) Prove Using reduction that state entry problem of Turing machines is undecidable. **(6)**

OR

14. (a) State and prove Rice's first theorem. **(8)**

(b) Prove Using reduction that whether a Turing Machine accepts empty string (or null string) is undecidable. **(6)**

15. (a) Show that the language $L = \{a^n b^n | n \geq 0\}$ can be decided by a deterministic Turing Machine in $O(n \cdot logn)$ time. **(7)**

(b) Let $t(n)$ be a function, where $n \in \mathbb{N}$ and $t(n) \geq n$. Then, prove that every $t(n)$ time nondeterministic single-tape Turing machine has an equivalent $2^{O(t(n))}$ time single-tape deterministic Turing machine. **(7)**

OR

16. (a) Prove that every context free language is a member of class P. **(8)**

(b) When is a problem said to be in class NP? **(6)**
Prove that Hamiltonian path problem of a directed graph is in class NP.

17. (a) Define Independent set in a graph. Prove that a graph G of n vertices with an independent set of size k contains a vertex cover of size $n - k$. **(8)**

(b) Define the complexity class NP Complete. Explain the significance of an NP Complete problem. **(6)**

OR

18. (a) Define the complement of a graph. Prove that the complement of a graph G of n vertices with a CLIQUE of size k contains an independent set of size k. **(7)**

(b) What is satisfiability problem. Prove that satisfiability problem is in class NP. **(7)**

19. (a) Illustrate Hamiltonian path in a Graph. **(4)**

(b) Prove that Hamiltonian path problem is in the class NP Complete. **(10)**

OR

20. (a) Prove that Vertex Cover problem is in the class NP Complete. **(8)**

(b) Why is it useful to identify that a problem is in the class NP Complete? **(6)**

Teaching Plan

No	Contents	No. of Lecture Hours (45 hrs)
Module-1(Overview of Automata Theory) (10 hours)		
1.1	Finite State Automata	1 hour
1.2	Push Down Automata	1 hour
1.3	Linear Bounded Automata	1 hour
1.4	Turing Machines	1 hour
1.5	Recursive Languages	1 hour
1.6	Recursively Enumerable Languages	1 hour
1.7	Universal Turing Machine	1 hour
1.8	Enumeration Machine	1 hour
1.9	Two Counter Machines	1 hour
1.10	Proof that two Counter Machines and Turing machines are equivalent	1 hour
Module-2 (Undecidability) (10 hours)		
2.1	Halting problem of Turing machine	1 hour
2.2	Proof of undecidability of Halting Problem	1 hour
2.3	Language representation of a problem	1 hour
2.4	Reduction	1 hour
2.5	Applications of reduction - Lecture 1	1 hour

2.6	Applications of reduction - Lecture 2	1 hour
2.7	Rice's First Theorem	1 hour
2.8	Proof of Rice's First Theorem	1 hour
2.9	Rice's Second Theorem	1 hour
2.10	Proof of Rice's Second Theorem	1 hour
Module-3 (Overview of Complexity Classes) (10 hours)		
3.1	Measuring time complexity, Asymptotic notations - Big O and small-o	1 hour
3.2	Analysing algorithms - time complexity class	1 hour
3.3	Complexity relationship among models - Single tape Turing Machine	1 hour
3.4	Multi-tape Turing Machine, Nondeterministic Turing Machine	1 hour
3.5	Class P	1 hour
3.6	Example problems in Class P	1 hour
3.7	Class NP	1 hour
3.8	Polynomial time verification	1 hour
3.9	Example problems in Class NP - Lecture 1	1 hour
3.10	Example problems in Class NP - Lecture 2	1 hour
Module-4 (NP Completeness) (9 hours)		
4.1	Satisfiability problem	1 hour
4.2	Polynomial time reducibility	1 hour
4.3	Overview of Graphs, CLIQUE, INDEPENDENT SET	1 hour
4.4	Vertex Cover	1 hour
4.5	Reducing 3SAT problem to CLIQUE - Lecture 1	1 hour
4.6	Reducing 3SAT problem to CLIQUE - Lecture 2	1 hour
4.7	NP Complete Problems	1 hour
4.8	Cook-Levin theorem, Proof - Lecture 1	1 hour
4.9	Proof - Lecture 2	1 hour
Module-5 (More NP Complete Problems) (6 hours)		

5.1	CLIQUE	1 hour
5.2	Vertex Cover - Lecture 1	1 hour
5.3	Vertex Cover - Lecture 2	1 hour
5.4	Hamiltonian path - Lecture 1	1 hour
5.5	Hamiltonian path - Lecture 2	1 hour
5.6	Hamiltonian path - Lecture 3	1 hour

		CATEGORY	L	T	P	CREDIT	YEAR OF INTRODUCTION
CST495	**CYBER FORENSICS**	**VAC**	**3**	**1**	**0**	**4**	**2019**

Preamble: The course on Cyber Forensics aims at exploring the basics of Cyber Forensics and Cyber security, the forensic investigation process and principles and the different types of cybercrimes and threats. This course also focuses on the forensic analysis of File systems, the Network, the Windows and Linux Operating systems. The course gives a basic understanding of the forensics analysis tools and a deep understanding of Anti forensics practices and methods. All the above aspects are dealt with case studies of the respective areas.

Prerequisite: Knowledge in File Systems, Operating systems, Networks and a general awareness on Cyber Technologies.

Course Outcomes: After the completion of the course the student will be able to

CO1	Explain thebasic concepts in Cyber Forensics, Forensics Investigation Process and Cyber security(**Cognitive Knowledge Level: Understand**)
CO2	Infer the basic concepts of File Systems and its associated attribute definitions (**Cognitive Knowledge Level: Understand)**
CO3	Utilize the methodologies used in data analysis and memory analysis for detection of artefacts**(Cognitive Knowledge Level: Apply)**
CO4	Identify web attacks and detect artefacts using OWASP and penetration testing. **(Cognitive Knowledge Level: Apply)**
CO5	Summarize anti-forensics practices and data hiding methods **(Cognitive Knowledge Level: Understand)**

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✓	✓				✓						✓
CO2	✓	✓										✓
CO3	✓	✓	✓	✓	✓							✓
CO4	✓	✓	✓	✓	✓							✓
CO5	✓	✓			✓							✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**		**End Semester Examination Marks**
	Test1 (Percentage)	**Test2 (Percentage)**	
Remember	30	30	30
Understand	40	40	40
Apply	30	30	30
Analyze			
Evaluate			
Create			

Mark Distribution

Total Marks	**CIE Marks**	**ESE Marks**	**ESE Duration**
150	50	100	3 hours

Continuous Internal Evaluation Pattern:

Attendance	: 10 marks
Continuous Assessment Tests	: 25 marks
Continuous Assessment Assignment	: 15 marks

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks.

First Internal Examination shall be preferably conducted after completing the first half of the syllabus and the Second Internal Examination shall be preferably conducted after completing remaining part of the syllabus.

There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly covered module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly covered module), each with 7 marks. Out of the 7 questions in Part B, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which a student should answer any one. Each question can have maximum 2 sub-divisions and carries 14 marks.

Syllabus

Module-1(Cyber Forensics and Cyber Security)

Computer Forensics: History of computer forensics, preparing for computer investigations, understanding Public and private investigations- Forensics Investigation Principles - Forensic Protocol for Evidence Acquisition - Digital Forensics -Standards and Guidelines - Digital Evidence – Data Acquisition - storage formats for digital evidence, determining the best acquisition method, contingency planning for image acquisitions, Cyber Forensics tools- Challenges in Cyber Forensics, Skills Required to Become a Cyber Forensic Expert

Cyber Security: Cybercrimes, Types of Cybercrimes - Recent Data Breaches - Recent Cyber security Trends - Case Study: Sim Swapping Fraud, ATM Card Cloning, Hacking email for money, Google Nest Guard, Email Crimes, Phishing, Types of Phishing.

Module-2 (File System Forensics)

File system Analysis: FAT and NTFS concepts and analysis -File system category, Content category, Metadata category, File name category, Application category,Application-level search techniques, Specific file systems, File recovery, Consistency check. FAT data structure-Boot sector, FAT 32 FS info, directory entries, Long file name directory entries

Module-3 (Operating System Forensics)

Windows Forensics: Live Response- Data Collection- Locard's Exchange Principle, Order of Volatility Volatile and Non Volatile Data Live-Response Methodologies: Data Analysis- Agile Analysis, Windows Memory Analysis, Rootkits and Rootkit detection.

Linux Forensics: Live Response Data Collection- Prepare the Target Media, Format the Drive, Gather Volatile Information, Acquiring the Image, Initial Triage, Data Analysis- Log Analysis, Keyword Searches, User Activity, Network Connections, Running Processes, Open File Handlers, The Hacking Top Ten, Reconnaissance Tools

Module-4 (Network Forensics)

The OSI Model, Forensic Footprints, Seizure of Networking Devices, Network Forensic Artifacts, ICMP Attacks, Drive-By Downloads, Network Forensic Analysis Tools, Case Study: Wireshark. Web Attack Forensics: OWASP Top 10, Web Attack Tests, Penetration Testing.

Module-5 (Anti-Forensics)

Anti-forensic Practices - Data Wiping and Shredding- Data Remanence, Degaussing, Case Study: USB Oblivion, Eraser - Trail Obfuscation: Spoofing, Data Modification, Case Study: Timestamp – Encryption, Case Study: VeraCrypt, Data Hiding: Steganography and Cryptography, Case Study: SilentEye, Anti-forensics Detection Techniques, Case Study: Stegdetect

Text Books

1. Bill Nelson, Amelia Phillips and Christopher Steuart, Computer forensics - Guide to Computer Forensics and Investigations, 4/e, Course Technology Inc.
2. Brian Carrier, File System Forensic Analysis, Addison Wesley, 2005.
3. Harlan Carvey, Windows Forensic Analysis DVD Toolkit, 2/e, Syngress.
4. Cory Altheide, Todd Haverkos, Chris Pogue,Unix and Linux Forensic Analysis DVD Toolkit, 1/e, Syngress.
5. William Stallings,Network Security Essentials Applications and Standards, 4/e, Prentice Hall
6. Eric Maiwald, Fundamentals of Network Security, McGraw-Hill, 2004.

References

1. Michael. E. Whitman, Herbert. J. Mattord, Principles of Information Security, Course Technology, 2011.
2. William Stallings, Cryptography and Network Security Principles and Practice, 4/e, Prentice Hall.
3. Niranjan Reddy, Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations, Apress, 2019.

Sample Course Level Assessment Questions

CourseOutcome1(CO1): Explain the Forensics principles and protocols for evidence acquisition.

Discuss the different cyber forensics tools used for image acquisition.

CourseOutcome2(CO2): Explain the pros and cons of NTFS and FAT File systems. Also give the challenges the investigators would face in extracting evidences from these file systems.

CourseOutcome3 (CO3): Apply any memory forensics methodologies/tools to extract volatile and nonvolatile data from a Windows based system.

CourseOutcome4 (CO4): Use web attacks test tools like netcraft to identify web application vulnerabilities of a particular site say **www.xyz.com**

Course Outcome 5 (CO5): Explain the different anti-forensics practices used to destroy or conceal data in order to prevent others from accessing it.

Model Question Paper

QP CODE:

Reg No: _______________

Name: ___________________ **PAGES : 3**

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: CST495

Course Name: Cyber Forensics

Max. Marks : 100 **Duration: 3 Hours**

PART A

Answer All Questions. Each Question Carries 3 Marks

1. Distinguish between public and private investigations.

2. What are the three computer forensics data acquisitions formats?

3. List any three features of NTFS which are not in FAT.

4. Define the terms file slack, RAM slack and drive slack.

5. What is Locard's exchange principle? Why is it important in forensic investigations?

6. Why would you conduct a live response on a running system?

7. What are the different tools used in Network Forensics?

8. Explain how Risk Analysis and Penetration Testing are different.

9. Why we are using Steganography?

10. How is data wiping done in hard drive?

(10x3=30)

Part B

(Answer any one question from each module. Each question carries 14 Marks)

11. (a) Discuss the different types of Cybercrimes. List the tools used for identifying Cyber Crimes. **(8)**

(b) Differentiate between Static acquisition and Live acquisition with example. **(6)**

OR

12. (a) Explain the principles of Digital Forensic Investigation? Why is it important? Comment. **(8)**

(b) When you perform an acquisition at a remote location, what should you consider preparing this task? **(6)**

13. (a) Discuss the FAT File Structure. **(8)**

(b) Does Windows NT use FAT or NTFS? Explain. **(6)**

14. (a) What is Metadata? Discuss the first 16 metadata records you would find in the MFT? **(6)**

(b) Explain the different data categories in a File System. **(8)**

15. (a) What is Agile requirement analysis? **(6)**

(b) Explain the different types of volatile information in a live response system. List any two tools used for obtaining volatile information. **(8)**

16. (a) What are the main live response methodologies? **(6)**

(b) What is Physical Memory Dump? Explain how a physical memory dump is analysed. **(8)**

17. (a) What is OWASP? Also mention the Top 10 web application vulnerabilities in 2021. **(8)**

(b) How would you setup Wireshark to monitor packets passing through aninternet router? **(6)**

18. (a) What are the goals of conducting a pentesting exercise? **(3)**

(b) Discuss the types of penetration testing methodologies. **(5)**

(c) Define OSI Layers. **(6)**

19. (a) How is Steganography done? **(7)**

(b) Why does data need Cryptography? **(4)**

(c) What is the difference between a Cryptographer and a Crypter? **(3)**

OR

20. (a) Explain the different types of Anti-forensics Detection Techniques. **(8)**

(b) What is Spoofing? How to prevent spoofing attack? **(6)**

TEACHING PLAN

Sl.No.	**Contents**	**No of Lecture Hrs (44hrs)**
	Module-1 (Cyber Forensics and Cyber Security) (11 Hrs)	
1.1	History of computer forensics, preparing for computer investigations	1 hour
1.2	Understanding Public and private investigations- Forensics Investigation Principles	1 hour
1.3	Forensic Protocol for Evidence Acquisition	1 hour
1.4	Digital Forensics -Standards and Guidelines - Digital Evidence	1 hour
1.5	Data Acquisition - storage formats for digital evidence, determining the best acquisition method	1 hour
1.6	Contingency planning for image acquisitions, Cyber Forensics tools	1 hour
1.7	Challenges in Cyber Forensics, Skills Required to Become a Cyber Forensic Expert	1 hour
1.8	Cybercrimes, Types of Cybercrimes - Recent Data Breaches - Recent Cyber security Trends	1 hour
1.9	Case Study: Sim Swapping Fraud, ATM Card Cloning	1 hour
1.10	Case Study:Hacking email for money, Google Nest Guard	1 hour
1.11	Email Crimes, Phishing, Types of Phishing	1 hour
	Module-2 (File System Forensics) (9 Hrs)	

2.1	FAT and NTFS concepts and analysis	1 hour
2.2	File system category, Content category	1 hour
2.3	Metadata category	1 hour
2.4	File name category,Application category	1 hour
2.5	Application-level search techniques	1 hour
2.6	Specific file systems, File recovery, Consistency check	1 hour
2.7	FAT data structure-Boot sector	1 hour
2.8	FAT 32 FS info, directory entries	1 hour
2.9	Long file name directory entries	1 hour
Module-3 (Operating System Forensics) (11 Hrs)		
3.1	Live Response- Data Collection- Locard's Exchange Principle	1 hour
3.2	Order of Volatility, Volatile and Non Volatile Data	1 hour
3.3	Live-Response Methodologies: Data Analysis- Agile Analysis	1 hour
3.4	Windows Memory Analysis	1 hour
3.5	Rootkits and Rootkit detection	1 hour
3.6	Linux Forensics: Live Response Data Collection	1 hour
3.7	Prepare the Target Media, Format the Drive, Gather Volatile Information	1 hour
3.8	Acquiring the Image, Initial Triage	1 hour
3.9	Data Analysis- Log Analysis, Keyword Searches, User Activity	1 hour

3.10	Data Analysis- Network Connections, Running Processes, Open File Handlers	1 hour
3.11	The Hacking Top Ten, Reconnaissance Tools	1 hour
Module-4 (Network Forensics) (7 Hrs)		
4.1	OSI Model	1 hour
4.2	Forensic Footprints, Seizure of Networking Devices, Network Forensic Artifacts	1 hour
4.3	ICMP Attacks, Drive-By Downloads, Network Forensic Analysis Tools	1 hour
4.4	Web Attack Forensics	1 hour
4.5	OWASP Top 10, Web Attack Tests	1 hour
4.6	Penetration Testing-1	1 hour
4.7	Penetration Testing.-2	1 hour
Module – 5 (Anti-Forensics) (6 Hrs)		
5.1	Anti-forensic Practices - Data Wiping and Shredding	1 hour
5.2	Data Remanence, Degaussing	1 hour
5.3	Trail Obfuscation: Spoofing, Data Modification	1 hour
5.4	Role of Encryption in Forensics	1 hour
5.5	Data Hiding: Steganography and Cryptography	1 hour
5.6	Anti-forensics Detection Techniques	1 hour

CST497	REINFORCEMENT LEARNING	CATEGORY	L	T	P	CREDIT	YEAR OF INTRODUCTION
		VAC	3	1	0	4	2019

Preamble: This course covers fundamental principles and techniques in reinforcement learning. Reinforcement learning is concerned with building programs that learn how to predict and act in a stochastic environment, based on past experience. Applications of reinforcement learning range from classical control problems, such as power plant optimization or dynamical system control, to game playing, inventory control, and many other fields. Topics include Markov decision process, dynamic programming, Monte Carlo, temporal difference, function approximation reinforcement learning algorithms, and applications of reinforcement learning. This course enables the leaners to apply reinforcement learning on real world applications and research problems.

Prerequisite: A pass in CST 294(Computational Fundamentals for Machine Learning)

Course Outcomes: After the completion of the course the student will be able to

CO 1	Solve computational problems using probability and random variables. **(Cognitive Knowledge Level: Apply)**
CO 2	Apply policy iteration and value iteration reinforcement learning algorithms. **(Cognitive Knowledge Level: Apply)**
CO 3	Employ Monte Carlo reinforcement learning algorithms. **(Cognitive Knowledge Level: Apply)**
CO 4	Apply temporal-difference reinforcement learning algorithms.(**Cognitive Knowledge Level: Apply)**
CO 5	Apply on-policy and off-policy reinforcement learning algorithms with function approximation. (**Cognitive Knowledge Level: Apply)**

Mapping of course outcomes with program outcomes

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
CO 1	✓	✓	✓									✓
CO 2	✓	✓	✓	✓								✓
CO 3	✓	✓	✓	✓								✓
CO 4	✓	✓	✓	✓								✓
CO 5	✓	✓	✓	✓	✓							✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**		**End Semester Examination**
	1	**2**	
Remember	**30%**	**30%**	**30%**
Understand	**30%**	**30%**	**30%**
Apply	**40%**	**40%**	**40%**
Analyse			
Evaluate			
Create			

Mark Distribution

Total Marks	**CIE Marks**	**ESE Marks**	**ESE Duration**
150	**50**	**100**	**3 hours**

Continuous Internal Evaluation Pattern:

Attendance	**: 10 marks**
Continuous Assessment Tests	**: 25 marks**
Continuous Assessment Assignment	**: 15 marks**

Internal Examination Pattern:

Each of the two internal examinations has to be conducted out of 50 marks

First Internal Examination shall be preferably conducted after completing the first half of the syllabus and the Second Internal Examination shall be preferably conducted after completing remaining part of the syllabus.

There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly covered module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly covered module), each with 7 marks. Out of the 7 questions in Part B, a student should answer any 5.

End Semester Examination Pattern: There will be two parts; Part A and Part B. Part A contain 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which student should answer anyone. Each question can have maximum 2 sub-divisions and carry 14 marks.

Syllabus

Module 1 (Review Of Probability Concepts)

Probability concepts review - Axioms of probability, concepts of random variables, probability mass function, probability density function, cumulative density functions, Expectation. Concepts of joint and multiple random variables, joint, conditional and marginal distributions. Correlation and independence.

Module 2 (Markov Decision Process)

Introduction to Reinforcement Learning(RL) terminology - Examples of RL, Elements of RL, Limitations and Scope of RL.

Finite Markov Decision Processes - The Agent–Environment Interface, Goals and Rewards, Returns and Episodes, Policies and Value Functions, Optimal Policies and Optimal Value Functions.

Module 3 (Prediction And Control)

Dynamic Programming - Policy Evaluation (Prediction), Policy Improvement, Policy Iteration, Value Iteration.

Monte Carlo (MC) for model free prediction and control - Monte Carlo Prediction, Monte

Carlo Estimation of Action Values, Monte Carlo Control, Monte Carlo Control without Exploring Starts, Off-policy Prediction via Importance Sampling, Incremental Implementation, Off-policy Monte Carlo Control.

Module 4 (Temporal-Difference (TD) Methods For Model Free Prediction And Control)

TD Methods - TD Prediction, Advantages of TD Prediction Methods, Optimality of TD(0), Sarsa: On-policy TD Control, Q-learning: Off-policy TD Control, Expected Sarsa.

n-step Bootstrapping- n-step TD Prediction, n-step Sarsa, step Off-policy Learning, Off-policy Learning Without Importance Sampling: The n-step Tree Backup Algorithm.

Module 5 (Function Approximation Method)

On-policy Prediction with Approximation - Value-function Approximation, The Prediction Objective, Stochastic-gradient Methods, Linear Methods.

Eligibility Traces - The λ-return, TD(λ), n-step Truncated λ-return Methods, Sarsa(λ).

Policy Gradient Methods - Policy Approximation and its Advantages, The Policy Gradient Theorem, REINFORCE: Monte Carlo Policy Gradient, REINFORCE with Baseline, Actor–Critic Methods.

Text book:

1 Richard S. Sutton and Andrew G. Barto, Reinforcement Learning: An Introduction, , 2nd Edition

2 Alberto Leon-Garcia, Probability, Statistics, and Random Processes for Electrical Engineering, 3rd Edition,

Reference books:

1 Reinforcement Learning: State-of-the-Art, Marco Wiering and Martijn van Otterlo, Eds

2 Algorithms for Reinforcement Learning, Szepesvari (2010), Morgan & Claypool.

3 Artificial Intelligence: A Modern Approach, Stuart J. Russell and Peter Norvig

4 Mathematical Statistics and Data Analysis by John A. Rice,University of California, Berkeley, Third edition, published by Cengage.

5 Machine Learning: A Probabilistic Perspective, Kevin P. Murphy

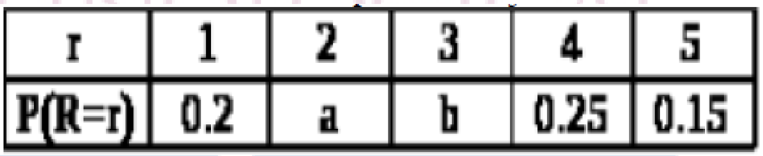
Sample Course Level Assessment Questions.

Course Outcome 1 (CO1):

1 Let ***J***and ***T***be independent events, where ***P(J)=0.4***and ***P(T)=0.7***. Find ***P(J ∩ T), P(J∪T)*** and ***P(J∩T')***

2 Let ***A*** and ***B*** be events such that ***P(A)=0.45*** , ***P(B)=0.35*** and ***P(A ∪B)=0.5***Find ***P(A | B)***

3 A random variable **R**has the probability distribution as shown in the following table:



r	1	2	3	4	5
P(R=r)	0.2	a	b	0.25	0.15

Given that ***E(R)=2.85***, find ***a*** and ***b***and ***P(R>2)***.

4 A biased coin (with probability of obtaining a head equal to ***p > 0***) is tossed repeatedly and independently until the first head is observed. Compute the probability that the first head appears at an even numbered toss.

5 Two players A and B are competing at a quiz game involving a series of questions. On any individual question, the probabilities that A and B give the correct answer are ***p*** and ***q*** respectively, for all questions, with outcomes for different questions being independent. The game finishes when a player wins by answering a question correctly. Compute the probability that A wins if

(i) A answers the first question,

(ii) B answers the first question.

6 A coin for which ***P(heads) = p***is tossed until two successive tails are obtained. Find the probability that the experiment is completed on the***n***thtoss.

7 An urn contains **p** black balls, **q** white balls, and **r** red balls; and **n** balls are chosen without replacement.

i. Find the joint distribution of the numbers of black, white, and red balls in the sample.

ii. Find the joint distribution of the numbers of black and white balls in the sample.

iii. Find the marginal distribution of the number of white balls in the sample.

8 Suppose that two components have independent exponentially distributed lifetimes, ***T1***and T2, with parameters ***α***and ***β***, respectively. Find (a) ***P(T1> T2)***and (b) ***P(T1> 2 T2)***.

9 Let ***Z1*** and ***Z2*** be independent random variables each having the standard normal distribution. Define the random variables ***X*** and ***Y*** by ***X = Z1 + 3Z2*** and Y = ***Z1+ Z2***. Argue that the joint distribution of ***(X, Y)*** is a bivariate normal distribution. What are the parameters of this distribution?

10 Given a continuous random variable ***x***, with cumulative distribution function ***Fx(x)***, show that the random variable ***y = Fx(x)*** is uniformly distributed.

11 ou roll a fair dice twice. Let the random variable ***X*** be the product of the outcomes of the two rolls. What is the probability mass function of ***X***? What are the expected values and the standard deviation of ***X***?

12 Show that if two events ***A***and ***B***are independent, then ***A***and ***B'***are independent

13 Prove that ***X***and ***Y***are independent if and only if ***fX|Y (x|y) = fX(x)***for all ***x***and ***y***

14 A random square has a side length that is a uniform [0, 1] random variable. Find the expected area of the square.Let X be a continuous random variable with the density function f (x) = 2x, 0 ≤ x ≤ 1

i. Find ***E(X)***.

ii. Find ***E(X^2)***and ***Var(X)***.

Course Outcome 2 (CO2):

1 What are the main differences between supervised learning and reinforcement learning?

2 Give examples of Markovian and non-Markovian environments?

3 What are the advantages and disadvantages of value methods vs policy methods?

4 Define the optimal state-value function **V^*(s)** for an MDP.

5 Imagine that the rewards are at most 1 everywhere. What is the maximum value that the discounted return can attain ? Why ?

6 Write down the Bellman optimality equation for state-value functions

7 Suppose that you are in a casino. You have Rs 20 and will play until you lose it all or as soon as you double your money. You can choose to play two slot machines: 1) slot machine A costs Rs 10 to play and will return Rs 20 with probability 0.05 and Rs 0 otherwise; and 2) slot machine B costs Rs 20 to play and will return Rs30 with probability 0.01 and Rs 0 otherwise. Until you are done, you will choose to play machine A or machine B in each turn. Describe the state space, action space, rewards and transition probabilities. Assume the discount factor γ = 1. Rewards should yield a higher reward when terminating with Rs 40 than when terminating with Rs 0. Also, the reward for terminating with Rs 40 should be the same regardless of how we got there (and equivalently for Rs 0).

Course Outcome 3 (CO3):

1 Explain policy iteration and value iteration? What are their similarities and differences?

2 Why Monte Carlo methods for learning value functions require episodic tasks? How is it that n-step TD methods avoid this limitation and can work with continuing tasks?

3 List any three uses of the depth parameter in the Monte-Carlo tree search procedure.

4 Given that $\mathbf{q_\pi(s, a) > v_\pi(s)}$, can we conclude that $\boldsymbol{\pi}$ is not an optimal policy. Justify

Course Outcome 4 (CO4):

1 Draw the backup diagram for 2-step Sarsa. Write the corresponding learning rule for 2-step Sarsa.

2 Why is Sarsa an on-policy algorithm while Q-learning is an off-policy algorithm?

3 How would you differentiate between learning algorithms using on-policy from those that use off-policy?

4 When using Temporal Difference learning, why is it better to learn action values (Q-values) rather than state values (V-values)?

5 Supose that a Q-learning agent always chooses the action which maximizes the Q-value. What is one potential problem with that approach?

6 Describe any two ways that will force a Q-learning agent to explore.

7 Why and when do we need importance sampling?

Course Outcome 5 (CO5):

1 How do you deal with a large possible action space in reinforcement learning?

2 List any two benefits of policy gradient methods over value function based methods.

3 What is the relation between Q-learning and policy gradients methods?

4 Consider a five state random walk. There are five states, $\mathbf{s_1, s_2, ..., s_5,}$ in a row with two actions each, left and right. There are two terminal states at each end, with a reward of **+1** for terminating on the right, after $\mathbf{s_5}$ and a reward of **0** for all other transitions, including the one terminating on the left after $\mathbf{s_1}$. In designing a linear function approximator, what is the least number of state features required to represent the value of the equi-probable random policy?

Model Question paper

QP Code : **Total Pages: 4**

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION (HONOURS), MONTH and YEAR

Course Code: CST497

Course Name: REINFORCEMENT LEARNING

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks.

1 The first three digits of a telephone number are 452. If all the sequences of the remaining four digits are equally likely, what is the probability that a randomly selected telephone number contains seven distinct digits?

2 If ***X*** is a discrete uniform random variable, i.e., ***P(X = k) = 1/n*** for ***k = 1, 2, ... , n***, find ***E(X)***and ***Var(X)***.

3 Define the discounted return $\mathbf{G_t}$. Give an expression for $\mathbf{G_t}$in terms of $\mathbf{G_{t+1}}$.

4 Write down the Bellman expectation equation for state-value functions.

5 Suppose that we are doing value iteration with $\gamma = 0$. How many iterations will it take for value iteration to converge to the optimal value function?

6 List any three advantages of Monte Carlo methods over dynamic programming techniques?

7 Draw the backup diagram for 2-step Q-learning. Write the corresponding learning rule for 2-step Q-learning.

8 Why Monte Carlo methods for learning value functions require episodic tasks. How does **n**-step TD methods avoid this limitation and can work with continuing tasks?

9 In using policy gradient methods, if we make use of the average reward formulation rather than the discounted reward formulation, then is it necessary to consider, for problems that do not have a unique start state, a designated start state, $\mathbf{s_0}$? Justify.

10 Value function based methods are oriented towards finding deterministic

policies whereas policy search methods are geared towards finding stochastic policies. True or false? Justify.

10 x 3 = 30

PART B

Answer any one Question from each module. Each question carries 14 Marks

11 a) Three players play 10 independent rounds of a game, and each player has probability 1/3 of winning each round. Find the joint distribution of the numbers of games won by each of the three players. **(7)**

b) Find the joint density of $\boldsymbol{X+Y}$ and $\boldsymbol{X/Y}$, where $\boldsymbol{X}$ and $\boldsymbol{Y}$ are independent exponential random variables with parameter $\boldsymbol{\lambda}$. Show that $\boldsymbol{X+Y}$ and $\boldsymbol{X/Y}$are independent. **(7)**

OR

12 a) An experiment consists of throwing a fair coin four times. Find the probability mass function and the cumulative distribution function of the following random variables: (7)

i the number of heads before the first tail

ii the number of heads following the first tail

iii the number of heads minus the number of tails

iv the number of tails times the number of heads.

b) Let $\boldsymbol{X}$ be a continuous random variable with probability density function on $\boldsymbol{0 <= x <= 1}$ defined by $\boldsymbol{f(x) = 3x^2}$. Find the pdf of $\boldsymbol{Y = X^2}$. **(7)**

13 a) What is the difference between a state value function **V(s)** and a state-action value function **Q(s,a)**? **(4)**

b) Consider designing a recycling robot whose job is to collect empty bottles around the building. The robot has a sensor to detect when a bottle is in front of it, and a gripper to pick up the bottle. It also senses the level of its battery. The robot can navigate, as well as pick up a bottle and throw a bottle it is holding in the trash. There is a battery charger in the building, and the robot should not run out of battery. **(10)**

i. Describe this problem as an MDP. What are the states and actions?

ii. Suppose that you want the robot to collect as many bottles as possible, while not running out of battery. Describe what rewards would enable it to achieve this task.

OR

14 a) Define the state-value function **$V_{\pi}(s)$** for a discounted MDP. **(5)**

b) Consider a 4x4 gridworld where the agent starts in the top left, the bottom rig state is terminal, rewards are always **-1**, **$\gamma = 1$**, and state transitions a deterministic. Consider the policy that always chooses the action to move dow except when it is on the bottom row, at which point it chooses the action to mov right. Starting with **$v_0(s) = 0$** for all **s**, compute **$v_1, v_2, \ldots, v_7$**. **(10)**

15 a) During a single iteration of the Value Iteration algorithm, we typically iterate over the states in **S** in some order to update **$V_t(s)$** to **$V_{t+1}(s)$** for all states **s**. Is it possible to do this iterative process in parallel? Explain why or why not. **(5)**

b) Consider an undiscounted Markov Reward Process with two states A and B. The transition matrix and reward function are unknown, but you have observed two sample episodes: **(9)**

A +3 --> A +2 --> B -4 --> A +4 --> B -3

B -2 --> A +3 --> B -3

i. Using first-visit Monte-Carlo evaluation, estimate the state-value function **V(A),V(B)**.

ii. Using every-visit Monte-Carlo evaluation, estimate the state-value function **V(A),V(B).**

iii. Draw a diagram of the Markov Reward Process that best explains these two episodes. Show rewards and transition probabilities on your diagram.

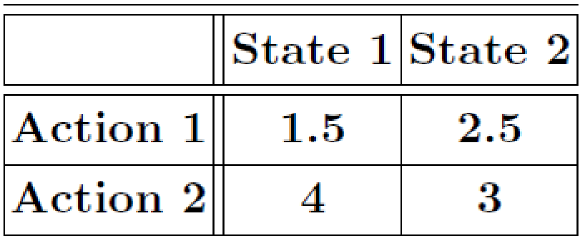
OR

16 a) Suppose you are given a finite set of transition data. Assuming that the Markov model that can be formed with the given data is the actual MDP from which the data is generated, will the value functions calculated by the MC and TD methods necessarily agree? Justify. **(4)**

b) With respect to the expected Sarsa algorithm, is exploration required as it is in the normal Sarsa and Q-learning algorithms? Justify. **(5)**

c) For a specific MDP, suppose we have a policy that we want to evaluate through the use of actual experience in the environment alone and using Monte Carlo methods. We decide to use the first-visit approach along with the technique of always picking the start state at random from the available set of states. Will this approach ensure complete evaluation of the action value function corresponding to the policy? **(5)**

17 a) Consider the following **Q[S,A]** table **(9)**



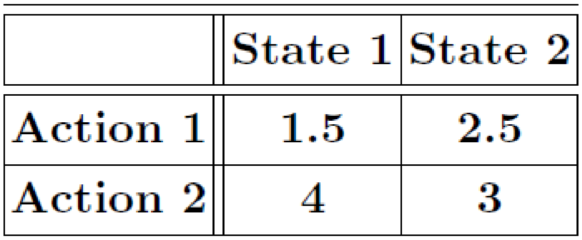
	State 1	State 2
Action 1	1.5	2.5
Action 2	4	3

Assume the discount factor, **γ= 0.5**, and the step size, **α = 0.1**. After the experience **(s, a, r, s')=(1, 1, 5, 2),** which value of the table gets updated and what is its new value?

b) What is the difference between Q-learning and Sarsa? **(5)**

OR

18 a) Consider the following **Q[S,A]** table **(9)**



	State 1	State 2
Action 1	1.5	2.5
Action 2	4	3

Assume the discount factor, **γ= 0.5**, and the step size, **α = 0.1**. After the experience **(s, a, r, s', a')=(1, 1, 5, 2, 1),** which value of the table gets updated and what is its new value?

b) For Q-learning to converge we need to correctly manage the exploration vs. exploitation tradeoff. What property needs to be hold for the exploration strategy? **(5)**

19 a) Given the following sequence of states observed from the beginning of an episode, $s_2, s_1, s_3, s_2, s_1, s_2, s_1, s_6$, what is the eligibility value, $e_7(s_1)$, of state $s_1$at time step 7 given trace decay parameter λ, discount rate γ, and initial value, $e_0(s_1) = 0$, when accumulating traces are used? What is the eligibility value if replacing traces are used? **(8)**

b) Suppose that we are using a policy gradient method to solve a reinforcement learning problem and the policy returned by the method is not optimal. Give three plausible reasons for such an outcome? **(6)**

OR

20 a) Suppose that we have a Q-value function represented as a sigmoid function of a set of features: **(8)**

$$Q(\phi, a) = \frac{1}{1 + e^{\theta^T \phi}}$$

Write down the update rule that Sarsa would give for this function.

b) Suppose that in a particular problem, the agent keeps going back to the same state in a loop. What is the maximum value that can be taken by the eligibility trace of such a state if we consider accumulating traces with **λ = 0.25** and **γ = 0.8**? **(6)**

Teaching Plan

No	Topic	No. of Lectures (42)
Module-1 (Review Of Probability Concepts) TB-2(Ch 2,3,4,5) (8 hours)		
1.1	Axioms of probability, concepts of random variables	1 hour
1.2	Probability mass function	1 hour
1.3	Probability density function	1 hour
1.4	Cumulative density functions	1 hour
1.5.	Expectation of random variables	1 hour
1.6.	Joint and multiple random variables	1 hour
1.7	Conditional and marginal distributions	1 hour
1.8	Correlation and independence	1 hour
Module-2 (Markov Decision Process) TB-1(Ch 1,3)(8 hours)		
2.1.	Introduction to Reinforcement Learning(RL) terminology - Examples of RL, Elements of RL, Limitations and Scope of RL	1 hour
2.2	Finite Markov Decision Processes	1 hour
2.3	The Agent–Environment Interface	1 hour
2.4.	Goals and Rewards	1 hour
2.5.	Returns and Episodes	1 hour
2.6.	Policies and Value Functions	1 hour
2.7	Optimal Policies and Optimal Value Functions	1 hour
2.8	Optimal Policies and Optimal Value Functions	1 hour
Module-3 (Prediction And Control) TB-1(Ch 4,5) (9 hours)		

3.1	Policy Evaluation (Prediction)	1 hour
3.2	Policy Improvement	1 hour
3.3	Policy Iteration, Value Iteration	1 hour
3.4	Monte Carlo Prediction	1 hour
3.5	Monte Carlo Estimation of Action Values	1 hour
3.6	Monte Carlo Control, Monte Carlo Control without Exploring Starts	1 hour
3.7	Off-policy Prediction via Importance Sampling	1 hour
3.8	Incremental Implementation	1 hour
3.9	Off-policy Monte Carlo Control	1 hour
Module-4 (Temporal-Difference(Td) Methods) TB-1 (Ch 6,7) (8 hours)		
4.1	TD Prediction, Advantages of TD Prediction Methods	1 hour
4.2	Optimality of TD(0)	1 hour
4.3	Sarsa: On-policy TD Control	1 hour
4.4	Q-learning: Off-policy TD Control	1 hour
4.5	Expected Sarsa	1 hour
4.6	n-step TD Prediction, n-step Sarsa	1 hour
4.7	n-step Off-policy Learning	1 hour
4.8	Off-policy Learning Without Importance Sampling: The n-step Tree Backup Algorithm	1 hour
Module-5 (Function Approximation Method) TB-1 (Ch 9,12,13) (9 hours)		
5.1	Value-function Approximation	1 hour
5.2	The Prediction Objective	1 hour
5.3	Stochastic-gradient Methods	1 hour
5.4	Linear Methods	1 hour
5.5	The Lambda-return , TD(Lambda)	1 hour
5.6	n-step Truncated Lambda-return Methods, Sarsa(Lambda)	1 hour
5.7	Policy Approximation and its Advantages	1 hour
5.8	The Policy Gradient Theorem, REINFORCE: Monte Carlo Policy Gradient	1 hour
5.9	REINFORCE with Baseline, Actor–Critic Methods	1 hour

CST499	**LOGIC FOR COMPUTER SCIENCE**	**CATEGORY**	**L**	**T**	**P**	**CREDIT**	**YEAR OF INTRODUCTION**
		VAC	**3**	**1**	**0**	**4**	**2019**

Preamble: This course enables the learners to understand the concepts of various logics used in computer science. The course covers the standard and most popular logics such as propositional logic, predicate logic, linear temporal logic, computation tree logic, Hoare logic and modal logic. This course helps the students to develop solutions for specification and verification of real world systems.

Prerequisite: Nil

Mapping of course outcomes with program outcomes

CO1	Explain the concepts of Predicate Logic, Propositional Logic, Linear Temporal Logic, Computation Tree Logic, Hoare Logic and Modal Logic as a formal language. **(Cognitive Knowledge Level: Understand)**
CO2	Develop proofs to show the satisfiability, validity and equivalence of logic formulas.**(Cognitive Knowledge Level: Apply)**
CO3	Illustrate model checking and program verification to prove correctness of systems.**(Cognitive Knowledge Level: Apply)**
CO4	Demonstrate *Alloy Analyzer* to model and analyze software systems. **(Cognitive Knowledge Level: Apply)**
CO5	Demonstrate *New Symbolic Model Verifier (NuSMV)* as a model checking tool to check the validity of temporal logic formulas.**(Cognitive Knowledge Level: Apply)**

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1	✓	✓	✓									✓
CO2	✓	✓	✓	✓								✓
CO3	✓	✓	✓	✓	✓							✓
CO4	✓	✓	✓	✓	✓							✓

CO5	✓	✓	✓	✓	✓							✓

Abstract POs defined by National Board of Accreditation			
PO#	**Broad PO**	**PO#**	**Broad PO**
PO1	Engineering Knowledge	**PO7**	Environment and Sustainability
PO2	Problem Analysis	**PO8**	Ethics
PO3	Design/Development of solutions	**PO9**	Individual and team work
PO4	Conduct investigations of complex problems	**PO10**	Communication
PO5	Modern tool usage	**PO11**	Project Management and Finance
PO6	The Engineer and Society	**PO12**	Life long learning

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**		**End Semester Examination Marks (%)**
	Test 1 (%)	**Test 2 (%)**	
Remember	**30**	**30**	**30**
Understand	**30**	**30**	**30**
Apply	**40**	**40**	**40**
Analyze			
Evaluate			
Create			

Mark Distribution

Total Marks	**CIE Marks**	**ESE Marks**	**ESE Duration**
150	**50**	**100**	**3**

Continuous Internal Evaluation Pattern:

Attendance	**10 marks**
Continuous Assessment Tests(Average of Internal Tests1&2)	**25 marks**
Continuous Assessment Assignment	**15 marks**

Internal Examination Pattern

Each of the two internal examinations has to be conducted out of 50 marks. First series test shall be preferably conducted after completing the first half of the syllabus and the second series test shall be preferably conducted after completing remaining part of the syllabus. There will be two parts: Part A and Part B. Part A contains 5 questions (preferably, 2 questions each from the completed modules and 1 question from the partly completed module), having 3 marks for each question adding up to 15 marks for part A. Students should answer all questions from Part A. Part B contains 7 questions (preferably, 3 questions each from the completed modules and 1 question from the partly completed module), each with 7 marks. Out of the 7 questions, a student should answer any 5.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 full questions from each module of which student should answer any one. Each question can have maximum 2 sub-divisions and carries 14 marks.

Syllabus

Module – 1 (Propositional Logic)

Declarative Sentences, Natural Deduction, Propositional Logic as a Formal Language, Semantics of Propositional Logic, Normal Forms, SAT Solvers.

Module– 2(Predicate Logic)

The Need of a Richer Language, Predicate Logic as a Formal Language, Proof Theory of Predicate Logic, Semantics of Predicate Logic, Undecidability of Predicate Logic, Expressiveness of Predicate Logic.

Module - 3 (Verification by Model Checking)

Motivation for Verification, Linear Time Temporal Logic (LTL), Model Checking Systems, Tools, Properties, Branching Time Logic, Computation Tree Logic (CTL) and the Expressive Powers of LTL and CTL, Model Checking Algorithms, The Fixed Point Characterization of CTL.

Module–4 (Program Verification)

Why Should We Specify and Verify Code, A Framework for Software Verification, Proof Calculus for Partial Correctness, Proof Calculus for Total Correctness, Programming by Contract.

Module–5 (Modal Logics and Agents)

Modes of Truth, Basic Modal Logic, Logic Engineering, Natural Deduction, Reasoning about Knowledge in a Multi-Agent System.

Text Books

1. Michael Huth and Mark Ryan, Logic in Computer Science, 2/e, Cambridge University Press, 2004.

Reference Books

1. Daniel Jackson, Software Abstractions, MIT Press, 2011.
2. Roberto Cavada, Alessandro Cimatti, Gavin Keighren, Emanuele Olivetti, Marco Pistore and Marco Roveri, NuSMV 2.6 Tutorial (available at *https://nusmv.fbk.eu*).
3. Tutorial for Alloy Analyzer 4.0 (available at *https://alloytools.org/tutorials/online/*).

Course Level Assessment Questions

Course Outcome1 (CO1):

1. Express the following statements as appropriate logic formulas.
    a. If the barometer falls, either it will rain or it will snow.
    b. No student attended every lecture.
    c. Once you are on the field, you keep on playing until the game is over.
    d. There are eight planets in the solar system.
2. Explain Horn Clause and Horn Formula.
3. Explain modal logic.

Course Outcome 2(CO2):

1. Prove the validity of the following sequents.

    $(p \wedge q) \wedge r, s \wedge t \vdash q \wedge s$

2. Prove the validity of

    (a) $\forall x \, \forall y \, P(x, y) \vdash \forall u \, \forall v \, P(u, v)$
    (b) $\exists x \, \exists y \, F(x, y) \vdash \exists u \, \exists v \, F(u, v)$
    (c) $\exists x \, \forall y \, P(x, y) \vdash \forall y \, \exists x \, P(x, y)$.

3. Prove that for all paths π of all models, $\pi \vDash \phi \, W \, \psi \wedge F \, \psi$ implies $\pi \vDash \phi \, U \, \psi$.

Course Outcome 3(CO3):

1. Consider an LTL formula $\phi \equiv (a\ U\ b) \longrightarrow F\ b$. Is ϕ valid? If yes, give an automata-theoretic proof of validity (i.e., construct a suitable NBA and use nested DFS to check an appropriate persistence condition). Otherwise, give a transition system that violates the formula. Illustrate the constructions clearly.

2. A familiar command missing from the core language (described in the text book) is the *for-statement*. It may be used to sum the elements in an array, for example, by programming as follows:

```
s = 0;
for (i = 0; i <= max; i = i+1) {
        s = s + a[i];
}
```

After performing the initial assignment s = 0, this executes i = 0 first, then executes the body *s = s + a[i]* and the incrementation *i = i + 1* continually until*i*<= *max* becomes false. Explain how ***for(C1;B;C2) {C3}*** can be defined as a derived program in our core language.

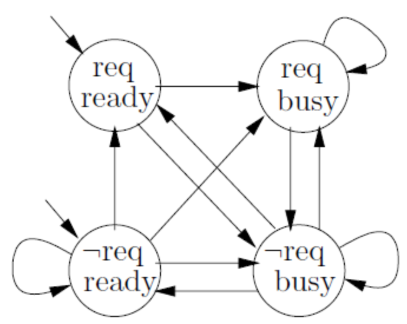
Course Outcome 4(CO4): .

1. Use *Alloy Analyzer* to model and solve the following problem.

A farmer is on one shore of a river and has with him a fox, a chicken, and a sack of grain. He has a boat that fits one object besides himself. In the presence of the farmer nothing gets eaten, but if left without the farmer, the fox will eat the chicken, and the chicken will eat the grain. How can the farmer get all three possessions across the river safely?

Course Outcome 5(CO5):

1. Simulate the following system using NuSMV..



Verify that $G\ (req\ \longrightarrow F\ busy)$ holds in all initial states.

Model Question Paper

QP CODE:

Reg No: _______________

Name: _________________ **PAGES : 4**

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: CST499

Course Name: Logic for Computer Science

Max.Marks:100 **Duration: 3 Hours**

PART A

Answer All Questions. Each Question Carries 3 Marks

1. Check the validity of the following sequents.
   a. $\sim p \longrightarrow \sim q \ \vdash q \longrightarrow p$
   b. $\sim(\sim p \vee q\ ) \ \vdash p)$

2. For the formula $\phi = p \wedge \sim(q \vee \sim p)$, we compute the inductively defined translation as $T(\phi) = p \wedge \sim\sim(\sim q \wedge \sim\sim p)$. Draw the parse tree of $T(\phi)$.

3. Translate the following into predicate logic.
   a. All red things are in the box.
   b. No animal is both a cat and a dog.

4. Let ϕ be $\exists x\ (P(y,z) \wedge\ (\forall y\ (\sim Q(y,x) \vee\ P(y,z))))$, where P and Q are predicate symbols with two arguments. Identify all bound and free variables in ϕ.

5. Show the syntax of Computation Tree Logic (CTL).

6. Prove that the LTL equivalence between $\phi\ U\ \psi$and$\sim\left(\sim\psi\ U\ (\sim\phi\ \wedge \sim\psi)\right) \wedge F\psi$.

7. Explain the need of specification and verification of code.

8. In what circumstances would $if\ (B)\{C1\}\ else\ \{C2\}$ fail to terminate?

9. Illustrate Kripke model.

10. With an example, explain the equivalences between modal formulas.

(10x3=30)

Part B

(Answer any one question from each module. Each question carries 14 Marks)

11. (a) Give the rules for Natural Deduction in propositional logic. **(6)**

(b) Use Natural Deduction to show the equivalence of the following formulas. **(8)**

a. $(p \wedge q) \wedge r, s \wedge t \vdash q \wedge s$

b. $(q \longrightarrow r) \longrightarrow ((\sim q \longrightarrow \sim p) \longrightarrow (p \longrightarrow r))$

OR

12. (a) What is a Horn Formula? How do you decide the satisfiability of a Horn formula. **(6)**

(b) Check the satisfiability of the following Horn Formulas. **(8)**

a. $(p \wedge q \wedge s \longrightarrow p) \wedge (q \wedge r \longrightarrow p) \wedge (p \wedge s \longrightarrow s)$

b. $(T \longrightarrow q) \wedge (T \longrightarrow s) \wedge (w \longrightarrow \perp) \wedge (p \wedge q \wedge s \longrightarrow v) \wedge (v \longrightarrow s) \wedge (T \longrightarrow r) \wedge (r \longrightarrow p)$

13. (a) Use Natural Deduction to prove the following equivalences. **(8)**

a. $\forall x(Q(x) \rightarrow R(x)), \exists x(P(x) \wedge Q(x)) \vdash \exists x(P(x) \wedge R(x))$

b. $\exists x P(x), \forall x(P(x) \longrightarrow Q(x)) \vdash \forall y Q(y)$

(b) Illustrate how Quantifier Equivalences can be used to check the equivalence of predicate logic formulas. **(6)**

OR

14. (a) Model the following system in *Alloy Analyzer*. **(7)**

There is an entity named **Person**, **Man** and **Woman** are two specializations of the entity **Person**. Every **Person** has a **Father** (a **Man**) and a **Mother** as **Parent**. The **Parent**s of a **Person** should be married. A **Man**'s **spouse** should be a **Woman** and a **Woman**'s **spouse** should be a **Man**. The **spouse** relation is symmetric.

Add a predicate to check whether marriage between siblings is possible in the above system.

(b) Explain Existential Second Order Logic and Universal Second Order Logic. **(7)**

15. (a) Model the Ferryman problem using New Symbolic Model Verifier (NuSMV). **(7)**

(b) Construct a Generalized Buchi Automaton for the LTL formula $\mathcal{O}a$. **(7)**

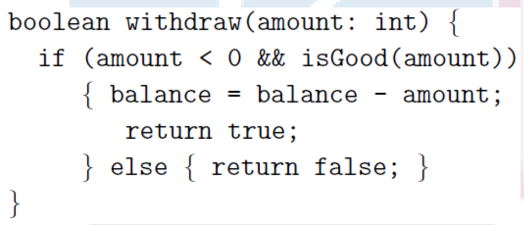
OR

16. (a) Show the closure of the LTL formula $\sim p\ U\ (F\ r \lor G \sim q \ \longrightarrow q\ W \sim r)$. **(7)**

(b) Explain the Fixed Point Characterization of CTL. **(7)**

17. (a) Illustrate partial correctness and total correctness in program verification. **(7)**

(b) **(7)**



```
boolean withdraw(amount: int) {
  if (amount < 0 && isGood(amount))
     { balance = balance - amount;
       return true;
     } else { return false; }
}
```

Consider the method named *withdraw* which attempts to withdraw amount from an integer field *balance* of the class within which the method *withdraw* lives. This method makes use of another method *isGood* which returns true iff the value of *balance* is greater than or equal to the value of *amount*.

Write a contract for the method *isGood*. Use that contract to show the validity of the contract for *withdraw*:

Method name: *withdraw*

Input: *amount* of type int

Assumes: *0 <= balance*

Guarantees: *0 <= balanace*

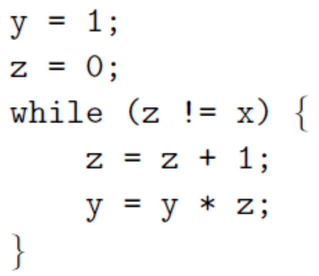
Output: of type boolean

Modifies only: *balance*

Upon validation, this contract establishes that all calls to *withdraw* leave *0<=balance* invariant.

OR

18. (a) Consider the program for computing the factorial of a number as given below. **(7)**

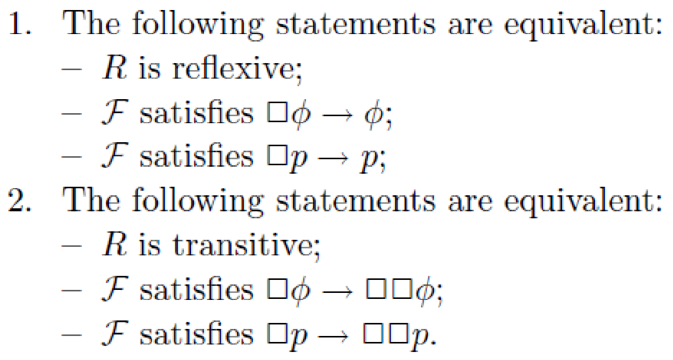


```
y = 1;
z = 0;
while (z != x) {
    z = z + 1;
    y = y * z;
}
```

Find a partial correctness proof for the above program.

(b) Explain the proof calculus for total correctness. **(7)**

19. (a) Let $\mathcal{F} = (W, R)$ be a frame. Prove the two claims given below. **(7)**



1. The following statements are equivalent:
   - R is reflexive;
   - $\mathcal{F}$ satisfies $\Box\phi \to \phi$;
   - $\mathcal{F}$ satisfies $\Box p \to p$;
2. The following statements are equivalent:
   - R is transitive;
   - $\mathcal{F}$ satisfies $\Box\phi \to \Box\Box\phi$;
   - $\mathcal{F}$ satisfies $\Box p \to \Box\Box p$.

(b) Explain the modal logics *K*, *KT45* and *KT4*. **(7)**

OR

20. (a) Prove the following using Natural Deduction. **(8)**

$\vdash_{\mathrm{KT45}} p \to \Box\Diamond p$, $\vdash_{\mathrm{KT45}} \Box\Diamond\Box p \to \Box p$

(b) Find a modal logic to formalize and solve *The Wise-Men Puzzle*. **(6)**

Teaching Plan

No	Contents	No. of Lecture Hours (45 hrs)
Module-1(Propositional Logic) (8 hours)		
1.1	Declarative Sentences, Natural Deduction	1 hour
1.2	Rule for Natural Deduction	1 hour
1.3	Derived Rules, Natural Deduction in Summary	1 hour
1.4	Provable Equivalence, Proof by Contradiction. Propositional Logic as a Formal language	1 hour
1.5	Semantics of Propositional Logic – The Meaning of Logical Connectives, Soundness of Propositional Logic, Completeness of Propositional Logic (Proof not required)	1 hour
1.6	Semantic Equivalence, Satisfiability and Validity	1 hour
1.7	Normal Forms – Conjunctive Normal Forms and Validity, Horn Clauses and Satisfiability	1 hour
1.8	SAT Solvers – A Linear Solver, A Cubic Solver	1 hour
Module-2(Predicate Logic) (7 hours)		
2.1	The Need of a Richer language, Predicate Logic as a Formal Language – Terms, Formulas, Free and Bound Variables, Substitution	1 hour
2.2	Proof Theory of Predicate Logic – Natural Deduction Rules	1 hour
2.3	Proof Theory of Predicate Logic – Quantifier Equivalences	1 hour
2.4	Semantics of Predicate Logic – Models, Semantic Entailment, The Semantics of Equality	1 hour
2.5	Undecidabilty of Predicate Logic (*no proof required*), Expressiveness of Predicate Logic – Existential Second Order Logic, Universal Second Order Logic	1 hour
2.6	Micromodels of Software – State Machines, A Software Micromodel (*Alloy*) (Lecture 1)	1 hour
2.7	A Software Micromodel (*Alloy*) (Lecture 2)	1 hour
Module-3(Verification by Model Checking) (13 hours)		

3.1	Motivation for Verification, Linear Time Temporal Logic (LTL) - Syntax	1 hour
3.2	Semantics of LTL – Practical Patterns of Specifications, Important Equivalences between LTL Formulas, Adequate Sets of Connectives for LTL	1 hour
3.3	Introduction to model checking	1 hour
3.4	Model Checking Systems, Tools, Properties	1 hour
3.5	Model checking example: Mutual Exclusion	1 hour
3.6	The New Symbolic Model Verifier (NuSMV) Model Checker – Introduction, Mutual Exclusion Revisited	1 hour
3.7	The NuSMV Model Checker – The Ferryman, The Alternating Bit Protocol	1 hour
3.8	Branching Time Logic – Syntax of Computation Tree Logic (CTL), Semantics of CTL	1 hour
3.9	Practical Patterns of Specification, Important Equivalences between CTL Formulas, Adequate Sets of CTL Connectives	1 hour
3.10	CTL and the Expressive Powers of LTL and CTL – Boolean Combinations of Temporal Formulas in CTL	1 hour
3.11	Model-Checking Algorithms – The CTL Model Checking Algorithm	1 hour
3.12	CTL Model Checking with Fairness	1 hour
3.13	The LTL Model Checking Algorithm (Algorithm only)	1 hour
Module-4 (Program Verification) (8 hours)		
4.1	Introduction to Program Verification, Need of Specification and Verification of Code	1 hour
4.2	A Framework for Software Verification – A Core Programming Language, Hoare Triples	1 hour
4.3	A Framework for Software Verification – Partial and Total Correctness, Program Variables and Logical Variables	1 hour
4.4	Proof Calculus for partial Correctness – Proof Rules	1 hour
4.5	Proof Calculus for partial Correctness – Proof Tableaux	1 hour
4.6	Proof Calculus for partial Correctness – A Case Study: Minimal-Sum Section	1 hour
4.7	Proof Calculus for Total Correctness	1 hour
4.8	Programming by Contract	1 hour
Module-5 (Modal Logics and Agents) (9 hours)		

5.1	Modes of Truth, basic Modal Logic - Syntax	1 hour
5.2	Basic Modal Logic - Semantics	1 hour
5.3	Logic Engineering – The Stock of Valid Formulas, Important Properties of the Accessibility Relation	1 hour
5.4	Logic Engineering – Correspondence Theory, Some Modal Logics	1 hour
5.5	Natural Deduction	1 hour
5.6	Reasoning about Knowledge in a Multi-Agent System –Examples (The Wise - Man Puzzle, The Muddy – Children Puzzle)	1 hour
5.7	The Modal Logic KT45n	1 hour
5.8	Natural Deduction for KT45n	1 hour
5.9	Formalizing the Examples (The Wise - Man Puzzle, The Muddy – Children Puzzle)	1 hour