Course work for IAI Ph.D. Students (Session: 2023-24)

The following courses will be offered to the first semester Ph.D. students of IAI.

- An: Analysis
- AA: Abstract Algebra
- LAMC: Linear Algebra & Multivariate Calculus
- To: Topolgy
- DM: Discrete Mathematics
- NT: Computational Number Theory
- PS: Probability and Statistics
- RM: Research Methodology
- Cr: Cryptology
- ML: Machine Learning
- AI: Artificial Intelligence
- PDS: An Introduction to Programming & Data Structures

The time table and details of each courses is given below.

<u>Time Table</u>

	10:00 - 11:30	11:30 - 13:00	14:30 - 16:00	16:00 - 17:30
Monday		DM / To	An / AI	Student Seminar
Tuesday	PS	Cr / To / ML	RM	PDS
Wednesday		DM / AA	NT / LAMC	Meet-in-the-Middle
Thursday	PS	AA / ML	RM	AI
Friday		Cr / LAMC	NT / An	PDS / Topology seminar

Course Name: Analysis

Instructor: Sayan Chakraborty

Teaching Assistant: Pratik Kumar Kundu

Syllabus:

Measure Theory:

1. Algebra, Sigma-algebra, Measurable sets

2. Measurable functions and their properties

3. Measure space, Lebesgue measure, product measure

4. Integration and convergence theorems

5. Introduction to L^p - spaces, Riesz-Fischer Theorem

6. Riesz representation theorem

Functional Analysis:

1. Normed linear spaces, Banach spaces, Hilbert Spaces

2. Bounded linear operators, compact operators on Hilbert spaces, spectral theorem

3. Hahn-Banach theorem and its applications, Open mapping and Closed graph theorem

References:

[1] G. B. Folland, Real Analysis: Modern Techniques and Their Applications, Wiley, 1999.

[2] John B Conway, A course in functional analysis, Second edition. Graduate Texts in Mathematics, 96. Springer-Verlag, New York, 1990

Course Name: Abstract Algebra

Instructor: Satyendra Mishra

Syllabus:

1. Quick Review of Basic Abstract Algebra: Groups, homomorphisms, normal subgroups and quotients, isomorphism theorems, finite groups, symmetric and alternating groups, direct product, structure of finite abelian groups, Sylow theorems. Rings and ideals, quotients, homomorphism and isomorphism theorems, maximal ideals, prime ideals, integral domains, field of fractions.

2. Factorization of polynomials: polynomials, fundamental theorem of algebra, the Euclidean algorithm, irreducibility, Gauss lemma, Eisenstein criterion, structure of finite fields, the multiplicative group.

3. Field automorphisms: the fundamental theorem of Galois theory, Galois extensions, Galois group, solvable groups, simple groups, solutions by radicals.

4. Field extensions: simple extensions, algebraic and transcendental extensions, algebraic closure; Minimal polynomials, simple algebraic extensions, the degree of an extension, splitting fields, normality and separability, Galois theory for abstract fields, transcendence degree, cyclic extensions.

5. Introduction to Module theory: modules, quotient modules and module homomorphisms, generation of modules, direct sums, and free modules, tensor products of modules, exact Sequences, Projective, Injective, and Flat modules.

References

[1] D. S. Dummit and R. M. Foote. Abstract algebra. John Wiley.

[2] I. N. Herstein Topics in Algebra. John Wiley.

[3] S. Lang. Algebra. GTM Springer. New York, 2011.

Course Name: Linear Algebra and Multivariable Calculus

Instructor: Suratno Basu and Somnath Hazra

Teaching Assistant: Saikat Goswami

Syllabus:

Linear Algebra

1. Vector spaces, Linear dependence, Basis, Linear Transformation, Eigenvalue and Eigenvector, Diagonalization.

2. Bilinear Forms, Symmetric Forms: Orthogonality, Hermitian Forms, The Spectral Theorem for Self-Adjoint and Normal Operators (In Finite Dimensional Cases), Sylvester's Law.

3. Jordan Canonical Form.

Multivariable Calculus

1. Differentiation, Partial Derivatives, Directional Derivatives, Jacobian Matrix, Chain Rule, Sufficient condition for differentiability and equality of mixed partial derivatives.

2. Inverse Functions, Implicit Functions

3. Differential Forms, Stoke's Theorem.

References:

[1] K. Hoffman and R. Kunze. Linear Algebra. Englewood Cliffs, NJ : Prentice-Hall,1971.

[2] Michael Artin. Algebra, Prentice Hall, 2000.

[3] M. Spivak. Calculus on Manifolds. CRC Press,1971.

[4] S. Lang. Calculus of several variables. Springer-Verlag. New York.

Course Name: Topology

Instructor: Kuldeep Saha

Teaching Assistant: Shital Lawande

Syllabus:

1. Topology of simplicial/cw/cell complexes and related notions of homotopy and quotient topology.

2. Fundamental Group and covering spaces.

3. Simplicial, singular and cellular versions of homology.

References:

[1] Algebraic Topology, Hatcher.

[2] Topology and Geometry, Bredon.

[3] Basic Topology, Armstrong

Course Name: Discrete Mathematics

Instructor: Subhabrata Samajder and Shion Samadder Chaudhury

Syllabus:

1. The Foundations – Logic and Proofs: Propositional logic, Predicates and Quantifiers, Rules of Inference, Proof methods and strategies.

2. Combinatorics: Sets, Functions, Relations, Equivalence relation, Partitions, PO Set, Lattice; Basics of counting, Pigeonhole principle, Permutation, Combination, Binomial and Multinomial Theorem, Generating permutation and combination, Inclusion-Exclusion and its application; Recurrence relation, Solving linear recurrence relation, Generating functions; Basic Number theory, Divisibility, Congruence, GCD, Euclidean Algorithm, Extended Euclidean Algorithm, Chinese Remainder theorem, RSA.

3. Graph Theory: Basic terminologies (clique, independent set, vertex cover, degree, regular, complement), Isomorphism, Algebraic Graph Theory, Representation of graphs, Connectivity, Eulerian paths and circuits, Hamiltonian paths and circuits, Knight's Tour; Graph traversal, Trees, Counting trees (Prufer Code), Minimal Spanning Trees, Planar graphs, Euler's Formula, Kuratowski's Theorem, Five-color Theorem, Bi-partite Matching, Halls Theorem, Stable Matching, Matching in any graph, Tutte's Theorem, Coloring of graphs, Chromatic Number, Brooks Theorem, Vizing's Theorem, Art Gallery Problem, products of graphs, strongly regular graphs, eigenvalues of graphs, evasive graph properties, expander graphs.

References:

[1] K. H. Rosen: Discrete Mathematics and Its Applications (8th Edition), McGraw Hill, 2019.

[2] N. L. Biggs: Discrete Mathematics, Clarendon Press, 1985.

[3] C. L. Liu: Elements of Discrete Mathematics, McGraw Hills, 1985.

[4] J. A. Bondy, U. S. R. Murty: Graph Theory, Graduate texts in mathematics 244, Springer, 2008.

[5] D. West: Introduction to Graph Theory, Prentice Hall, 2000.

[6] R. Diestel: Graph Theory, Graduate texts in mathematics 173, Springer-Verlag Berlin Heidelberg, 2017.

[7] B. Bollobas: Modern Graph Theory, Graduate texts in mathematics, Springer, 2002.

Course Name: Computational Number Theory

Instructor: Rana Barua and Avik Chakraborti

Syllabus:

1. Integer Arithmatic: Divisibility, Greatest Common Divisor, Euclidean and Extended Euclidean Algorithm, modular arithmetic, modular exponentiation, Montgomery arithmetic, Congruences, Chinese Remainder Theorem, Orders and Primitive Roots, Euler’s Phi function, Euler’s Theorem, Fermat’s little theorem, Quadratic Residue, Distribution of Primes, Sieves of Eratoshthenes, Prime number theorem

2. Representation of finite fields: Prime and extension fields, representation of extension fields, polynomial basis, primitive elements, irreducible polynomials.

3. Algorithms for polynomials: Root-finding and factorization, Lenstra-Lenstra-Lovasz algorithm, polynomials over finite fields.

4. Elliptic curves: The elliptic curve group, elliptic curves over finite fields, Schoof's point counting algorithm.

5. Primality testing algorithms: Fermat test, Miller-Rabin test, Solovay-Strassen test, AKS test.

6. Integer factoring algorithms: Trial division, Pollard rho method, p-1 method, CFRAC method.

7. Computing discrete logarithms over finite fields: Baby-step-giant-step method, Pollard rho method, Pohlig-Hellman method

References:

[1] A. Das, Computational number theory, Chapman and Hall/CRC.

[2] V. Shoup, A computational introduction to number theory and algebra, Cambridge University Press.

[3] H. Cohen, A course in computational algebraic number theory, Springer-Verlag.

Course Name: Elements of Probability and Statistics

Instructor: Avisek Gupta and Swagatam Das

Syllabus:

1. Introduction to Probability: Sample space, events, probability axioms, Conditional probability and Bayes' theorem, Independence and random variables, Probability distributions: Discrete and continuous

2. Common Probability Distributions: Bernoulli, Binomial, and Poisson distributions; Uniform, Normal (Gaussian), and Exponential distributions, Gamma and Weibull distributions

3. Elementary probability inequalities and concentration of measures.

4. Descriptive statistics: Measures of central tendency and dispersion Data visualization: Histograms, box plots, and scatter plots Exploratory Data Analysis (EDA) techniques

5. Statistical Inference I: Sampling distributions and the Central Limit Theorem, Confidence intervals for population parameters, Hypothesis testing: One-sample and two-sample tests.

6. Statistical Inference II: Analysis of Variance (ANOVA), Chi-square tests for independence Nonparametric tests: Wilcoxon rank-sum test, Kruskal-Wallis test

7. Regression Analysis: Simple linear regression, Multiple linear regression, Model selection and diagnostics.

8. Rudiments of Bayesian Statistics: Bayes' theorem and Bayesian updating, Bayesian parameter estimation and credible intervals, Bayesian hypothesis testing and decision making.

9. Introduction to Time Series Analysis: Time series components and decomposition, Autoregressive (AR) and Moving Average (MA) models, Forecasting techniques for engineering applications.

References:

[1] Douglas C. Montgomery and George C. Runger, Applied Statistics and Probability for Engineers, John Wiley & Sons, Limited, 2014.

[2] Douglas C. Montgomery, George C. Runger, Norma F. Hubele, Engineering Statistics, 5th Edition, Wiley

Course Name: Research Methodology

Instructor: Arpita Maitra and Rana Barua

Syllabus:

1. Fundamentals of Research Basics: Definition, Purpose and Classification of research, Fundamentals of research methods, Writing a research proposal; Problem Identification: Review of literature, Broadening knowledge base in the specific research area, Bringing clarity and focus to the research problem, Writing a research proposal, Writing research reports/papers; Identifying variables: The difference between a concept and a variable, Converting concepts into variables, Types of variable, Types of measurement scale.

2. Research Design Selecting a study design: Differences between quantitative and qualitative study designs, Study designs in quantitative research, Data collection: Selecting a method of data collection, Differences in the methods of data collection in quantitative and qualitative research, Major approaches to information gathering, Methods of data collection in qualitative research.

3. Fundamentals of Statistics: Frequency, Measure of Central Tendency, Dispersion, Regression and Interpretation of Results.

4. Basics of Probability: Definition of Probability, Conditional Probability, Bayes' Random Variable, Probability Distribution.

5. Optimization Techniques: Maxima & Minima, Condition of Optimality, Linear Programming Problem (Introduction, Formation of LPP, Graphical method of solution).

References:

[1] Research Methodology Methods & Techniques, C. R. Kothari, New Age International (P) Limited, Publisher, 2004.

[2] Research Methodology: A Step-by-Step Guide for Beginners (Fourth Edition), Ranjit Kumar, SAGE publishing, 2015.

[3] Fundamental of Research Methodology and Statistics, Y.K. Singh, New Age International (P) Limited, 2006.

[4] Research Methods and Statistics: A Critical Thinking Approach, Sherri L Jackson, American Psychological Association, 5th edition, Cengage Learning, 2014.

Course Name: Cryptology

Instructor: Dr. Nilanjan Datta and Dr. Subhabrata Samajder

Teaching Assistant: Hrithik Nandi and Mriganka Dey

Syllabus:

1. Introduction: Classical Ciphers, Shannon Cipher, Perfect Security, Computational Ciphers and Semantic Security.

2. Encryption: Stream Ciphers, Pseudo random generators, LFSR based stream ciphers, RC4 and its Cryptanalysis; Block ciphers: Design principle, AES and its design rationale, light-weight block cipher design; Security Notions, Modes of operation: ECB, CBC, OFB, Counter mode.

3. Cryptanalysis: Goal and power of an adversary; Differential and Linear Cryptanalysis; Some advanced cryptanalysis (integral, impossible differential) and its applications.

4. Hash Function: Collision resistant (CR) hash functions, birthday attacks CR hash, The Merkle-Damgard paradigm, Joux's multi-collsion attacks; Universal hash functions (UHF), constructing UHFs.

5. Message Integrity: Message authentication codes (MACs); Designing MACs from CR hash, Case Study: HMAC, Sponge based MACs; Designing MACs from UHF, The Carter-Wegman MACs, Nonce based MACs.

6. Authenticated Encryption (AE): Motivation, Security, Designing AE: Generic Paradigm, Integrated AE; Features of AE, Light-weight AE design.

7. Public Key Cryptosystems: Discrete Logarithm Problem, Diffie Hellman Key Exchange Protocol - security proofs and some related hardness results on CDH and DDH, RSA Encryption and Its variants, Elgamal Encryption Scheme, Digital Signatures - Attacks on Plain RSA signatures, Full Domain RSA, Identification Scheme, Fiat-Shamir Transform, Schnorr Signatures, DSA and ECDSA, PKI.

References:

[1] D. Boneh, V. Shoup: A Graduate Course in Applied Cryptography.

[2] J. Katz and Y. Lindell: Introduction to Modern Cryptography, Chapman & Hall/CRC, 2007.

[3] K. Sakiyama, Y. Li and Y. Sasaki: Security of Block Ciphers: From Algorithm Design to Hardware Implementation, Published by Wiley & Sons, Incorporated, John, 2016. ISBN 10: 1118660013.

[4] V. Shoup: A Computational Introduction to Number Theory and Algebra, Cambridge University Press.

Course Name: Introduction to Machine Learning

Instructor: Md Sahidullah

Syllabus:

1. Machine learning basics: Elementary concepts of learning systems, data, information, and knowledge, machine learning workflow and terminologies (feature extraction, modeling, training, validations, evaluations), different kinds of machine learning – supervised, unsupervised, reinforcement learning, concepts of training and testing data, overview of applications.

2. Evaluation metrics: Accuracy, precision, recall, F-score, AUC, ROC, mean squared error.

3. Supervised Learning: Regression – linear regression, classification – logistic regression, nearest neighbor classifier, naïve Bayes classifier, support vector machines, decision trees, ensemble classifiers – bagging (random forest) and boosting.

4. Unsupervised Learning: Clustering (k-means and simple hierarchical clustering algorithms), principal component analysis, t-distributed stochastic neighbor embedding, non-negative matrix factorization, maximum likelihood estimates.

5. Neural networks: Perceptron, universal approximation theorem, multi-layer perceptron, gradient descent algorithm, autoencoder, introduction to recurrent neural network.

6. Issues in machine learning: Generalization, overfitting, regularization, empirical risk minimization, cross-validation, curse of dimensionality, imbalanced data.

7. Machine learning applications: Case studies of machine learning applications in computer vision, speech and natural language processing.

References:

[1] Duda, R.O., Hart, P.E., Strok, D.G., 2006. Pattern Classification. John Wiley & Sons.

[2] Bishop, C.M., 2006. Pattern Recognition and Machine Learning. Springer.

[3] Mitchell, T.M.,, 2017. Machine Learning, McGraw Hill Education.

Course Name: Artificial Intelligence

Instructor: Narayan Changder

Syllabus:

1. Overview of Artificial intelligence - Problems of AI, AI technique, Tic - Tac - Toe problem.

2. Agents & environment, nature of environment, structure of agents, goal based agents, utility based agents, learning agents. Agents' coalition formation.

3. Defining the problem as state space search, production system, problem characteristics, issues in the design of search programs.

4. Solving problems by searching: problem solving agents, searching for solutions; uniform search strategies: breadth first search, depth first search, depth limited search, bidirectional search, comparing uniform search strategies.

5. Greedy best-first search, A* search, memory bounded heuristic search: local search algorithms & optimization problems: Hill climbing search, simulated annealing search, local beam search, genetic algorithms; constraint satisfaction problems, local search for constraint satisfaction problems.

6. Games, optimal decisions & strategies in games, the minimax search procedure, alpha-beta pruning, additional refinements, iterative deepening.

7. Knowledge representation issues, representation & mapping, approaches to knowledge representation, issues in knowledge representation.

8. Representing simple fact in logic, representing instant & ISA relationship, computable functions & predicates, resolution, natural deduction.

9. Procedural verses declarative knowledge, logic programming, forward verses backward reasoning, matching, control knowledge.

10. Components of a planning system, Goal stack planning, Hierarchical planning, other planning techniques.

11. Syntactic processing, semantic analysis, discourse & pragmatic processing.

12. Representing and using domain knowledge, expert system shells, knowledge acquisition.

References:

[1] Artificial Intelligence, Ritch & Knight, TMH

[2] Artificial Intelligence A Modern Approach, Stuart Russel Peter Norvig Pearson

[3] Introduction to Artificial Intelligence & Expert Systems, Patterson, PHI

Course Name: Introduction to Programming and Data Structure

Instructor: Laltu Sardar and Ritankar Mondal

Syllabus:

1. The Evolution of Programming Languages, Compiler, Interpreter, Assembler

2. Imperative languages: Introduction to imperative language; syntax and constructs of a specific language (preferably C)

3. Variables, assignments, Basic input/output, Main program, If-statement, Logical operators, Loops, Output formatting, Parameters, return values, Debugger

4. Arrays, Pointers, Dynamic Memory Allocation, Structures

5. Basic structures: Lists, Strings, Dictionary, Values and references

6. Basics of program design, Programming style, Exceptions

7. Functions and Recursion: Parameter passing, procedure call, call by value, call by reference, recursion, scope of variables.

8. Linked lists: Implementation of linked lists, inserting, deleting, and inverting a linked list, Stacks and Queues.

9. Matrix Algorithms: Matrix addition, multiplication, and inverse calculation. Finding Eigen values and Eigen vectors. Efficient Algorithms for large/sparse matrices.

10. Algorithm for Polynomials: Polynomial addition and multiplication, division.

11. File handling: principles of data storage and manipulation

12. Matrix Algorithms: Finding Eigen values and Eigen vectors of a large Matrix. Polynomial addition and multiplication.

References:

[1] B. W. Kernighan and D. M. Ritchi: The ‘C’ Programming Language, Prentice Hall, Englewood Cliffs, NJ, 1980.

[2] B. Gottfried: Programming in C, Schaum Outline Series, New Delhi, 1996.

[3] D. E. Knuth: The Art of Computer Programming. Vol. 1, 2nd ed. Narosa/Addison-Wesley, New Delhi/London, 1973.