Computer Sc. & Engg. Deptt.
M. Tech in Computer Science & Engineering

Semester 1

Subject	L-T-P	Credits
CS60001 Foundations of Computing Science	3-1-0	4
CS60003 Algorithm Design and Analysis	4-0-0	4
Elective 1	3-0-0	¾
Elective 2	3-0-0	¾
Elective 3 (HSS /MGMT/Depth optional)	3-0-0	¾
CS69011 Computing Lab 1	0-0-6	4
CS69001 Seminar 1	0-0-3	2
Total:		23/26

Semester 2

Subject	L-T-P	Credits
Core 3 High Performance Computer Arch.	4-0-0	4
Elective 4	3-0-0	3
Elective 5	3-0-0	3/4
Elective 6	3-0-0	3/4
Elective 7	3-0-0	3/4
CS69012 Computing Lab 2	0-0-6	4
CS69002 Seminar 2	0-0-3	2
Total:		22/25

Total Credit of Lecture Courses: 33-40

Semester 3

Subject	L-T-P	Credits
CS67001 Project		20
CS68002 Comprehensive Viva Voce		3
Total:		23

Semester 4

Sub. No.	Subject	L-T-P	Credits
CS67002	Project		20
	Total:		20

Out of 20 credit in Project, 4 credits for project work during Summer vacation (from May to July)

Total Credit: 88-94

List of Autumn (Odd) Semester Electives

Sub. No.	Subject	L-T-P	Credits	Prerequisites
CS 60031	Logics for Computer Science	3-1-0	4	Discrete Structure
CS 60033	Logic Programming	3-0-0	3	
CS 60035	Information Retrieval	3-0-0	3	
CS 60037	Embedded Systems	3-1-0	4	Computer Orgn. & Arch. Operating System
CS 60039	Testing and Verification of Circuits	3-1-0	4	Switching Ckts & Logic Design/ Dig. Electronics
CS 60041	Cryptography & Network Security	3-1-0	4	Algorithms I & Discrete Strc.
CS 60043	Algorithms for Bioinformatics	3-0-0	3	Algorithms I
CS 60045	Artificial Intelligence	3-0-0	3	Algorithms I
CS 60047	Advanced Graph Theory	3-1-0	4	Disc. Strct & Algo I
CS 60049	Computational Complexity	3-1-0	4	Disc. Strct. & Algo I
CS 60051	Discrete Structures	3-1-0	4	
CS 60053	VLSI System Design	3-1-0	4	Switching Ckts & Logic Design/ Dig. Electronics
CS 60055	Ubiquitous Computing	3-0-0	3	Computer Ntks.
CS 60057	Speech & Natural Lang. Proc.	3-0-0	3	
CS 60059	Object Oriented Systems	3-0-0	3	Software Eng. + Lab
IT60107	Data Warehousing & Data Mining	4-0-0	4	
IT60109	Cluster and Grid Computing	3-0-0	3	

List of Spring (even) Semester Electives

Sub. No.	Subject	L-T-P	Credits	Prerequisites
CS 60030	Distributed Systems	4-0-0	4	
CS 60032	Database Engineering	3-0-0	3	DBMS
CS 60034	Advanced Microprocessor Based Systems	3-0-0	3	Comp. Org & Arch + lab
CS 60036	Intelligent Systems	3-0-0	3	Algorithm I
CS 60038	Advances in Operating Systems Design	3-0-0	3	OS + Lab.
CS 60040	Parallel & Distributed Algorithms	3-0-0	3	Algorithm I + Comp. Org. Arch.
CS 60042	Advances in Compiler Construction	3-1-0	4	Compiler + Lab
CS 60044	Perf. Eval. & Reliability of Information Sys.	3-0-0	3	Probability + Stat.
CS 60046	Real Time Systems	3-0-0	3	OS + Lab
CS 60048	Theory of Programming Languages	3-0-0	3	Disc. Strct.
CS 60050	Machine Learning	3-0-0	3	Artf. Intel.
CS 60052	Advanced Digital Img Proc & Comp Vision	3-0-0	3	Disc. Strct. + Signals & Networks + Lab
CS 60054	Low Power Circuits Design	3-0-0	3	VLSI Syst. Design
CS 60056	Computer Graphics	3-1-0	4	Algo I + Lab
CS 60058	Fault Tolerant Systems	3-0-0	3	
CS 60060	Formal Systems	3-1-0	4	
CS 60062	Multimedia Systems	3-0-0	3	Image Proc.
CS 60064	Computational Geometry	3-1-0	4	Algo I + Lab
CS 60066	Software Engineering	3-0-3	5	Disc. Strct.
CS 60068	CAD for VLSI Design	3-1-0	4	Algo I + Lab. Com Org Arch +

				Lab
CS 60070	Quantum Computing & Quantum Inf. Proc.	3-1-0	4	
CS 60076	Advances in Digital and Mixed Signal Testing	3-0-0	3	
CS 60078	Complex Networks	3-0-0	3	Algo I + Lab.
CS 60080	Selected Topics in algorithms	3-0-0	3	Algorithms I + Algorithms Lab
CS 60082	Computational Number Theory	3-0-0	3	
CS 60084	Foundations of Cryptography	3-1-0	4	
CS 63052	Information Technology	3-0-3	5	(only for MMST students)
IT 60004	E-Commerce	4-0-0	4	
IT 60030	Information System Design	4-0-0	4	

Computer Science and Engineering Department

Syllabi of M.Tech. Subjects

CS60001 Foundations of Computing Science L-T-P: 3-1-0, Credit: 4

Discrete Structures -- Sets, Relations and Functions; Proof Techniques, Algebraic Structures, Morphisms, Posets, Lattices and Boolean Algebras.
Logic -- Propositional calculus and Predicate Calculus, Satisfiabiliy and validity, Notions of soundness and completeness
Languages & Automata Theory -- Chomsky Hierarchy of Grammars and the corresponding acceptors, Turing Machines, Recursive and Recursively Enumerable Languages; Operations on Languages, closures with respect to the operations.
Computability -- Church-Turing Thesis, Decision Problems, Decidability and Undecidability, Halting Problem of Turing Machines; Problem reduction (Turing and mapping reduction).
Computational Complexity -- Time Complexity -- Measuring Complexity, The class P, The class NP, NP-Completeness, Reduction, co-NP, Polynomial Hierarchy. Space Complexity -- Savich's Theorem, The class PSPACE.

Text Books and References:

1. J.P. Trembley and R. Manohar -- Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill Book Co.,

2. Michael Sipser -- Introduction to The Theory of Computation, Thomson Course Technology.

3. John E. Hopcroft and J.D.Ullman -- Inrtroduction to Automata Theory, Languages and Computation, Narosa Pub. House, N. Delhi.

4. H.R. Lewis and C.H.Papadimitrou -- Elements of the Theory of Computation, Prentice Hall, International, Inc.

CS 60003 Algorithm Design and Analysis L-T-P: 4-0-0, Credit: 4

Algorithmic paradigms: Dynamic Programming, Greedy, Branch-and-bound; Asymptotic complexity, Amortized analysis; Graph Algorithms: Shortest paths, Flow networks; NP-completeness; Approximation algorithms; Randomized algorithms; Linear programming; Special topics: Geometric algorithms (range searching, convex hulls, segment intersections, closest pairs), Numerical algorithms (integer, matrix and polynomial multiplication, FFT, extended Euclid's algorithm, modular exponentiation, primality testing, cryptographic computations), Internet algorithms (text pattern matching, tries, information retrieval, data compression, Web caching).

CS 60002 High Performance Computer Architecture L-T-P: 4-0-0, Credit: 4

Introduction: review of basic computer architecture, quantitative techniques in computer design, measuring and reporting performance. CISC and RISC processors. Pipelining: Basic concepts, instruction and arithmetic pipeline, data hazards, control hazards, and structural hazards, techniques for handling hazards. Exception handling. Pipeline optimization techniques. Compiler techniques for improving performance. Hierarchical memory technology: Inclusion, Coherence and locality properties; Cache memory organizations, Techniques for reducing cache misses; Virtual memory organization, mapping and management techniques, memory replacement policies. Instruction-level parallelism: basic concepts, techniques for increasing ILP, superscalar, superpipelined and VLIW processor architectures. Array and vector processors. Multiprocessor architecture: taxonomy of parallel architectures. Centralized shared-memory architecture: synchronization, memory consistency, interconnection networks. Distributed shared-memory architecture. Cluster computers. Non von Neumann architectures: data flow computers, reduction computer architectures, systolic architectures.

CS 60030 Distributed Systems L-T-P: 4-0-0, Credit: 4

Basic concepts. Models of computation: shared memory and message passing systems, synchronous and asynchronous systems. Logical time and event ordering. Global state and snapshot algorithms, mutual exclusion, clock synchronization, leader election, deadlock detection, termination detection, spanning tree construction. Programming models: remote procedure calls, distributed shared memory. Fault tolerance and recovery: basic concepts, fault models, agreement problems and its applications, commit protocols, voting protocols, checkpointing and recovery, reliable communication. Security and Authentication: basic concepts, Kerberos. Resource sharing and load balancing. Special topics: distributed objects, distributed databases, directory services, web services.

CS 60031 Logics for Computer Science L-T-P: 3-1-0, Credit: 4

Axiomatic Theory: Propositional Calculus, Predicate Calculus, First Order Theories, Peano Arithmetic. Decision Procedures in First Order Logic: Resolution Theorem Provers: some theoretical issues. Modal Logic, Temporal Logic: their applications, Model Checking. Model Theory, Proof Theory. mu Calculus, Lambda Calculus, Non-monotonic Reasoning, Intuitionistic First Order Logic, Fuzzy Logic.

CS 60032 Database Engineering L-T-P: 3-0-0, Credit: 3

Relational Databases: Integrity Constraints revisited: Functional, Multi-valued and Join Dependency, Template Algebraic, Inclusion and Generalized Functional Dependency, Chase Algorithms and Synthesis of Relational Schemes. Query Processing and Optimization: Evaluation of Relational Operations, Transformation of Relational Expressions, Indexing and Query Optimization, Limitations of Relational

Data Model, Null Values and Partial Information. Deductive Databases: Datalog and Recursion, Evaluation of Datalog program, Recursive queries with negation. Objected Oriented and Object Relational Databases: Modeling Complex Data Semantics, Specialization, Generalization, Aggregation and Association, Objects, Object Identity, Equality and Object Reference, Architecture of Object Oriented and Object Relational Databases. Case Studies: Gemstone, O2, Object Store, SQL3, Oracle xxi, DB2. Parallel and Distributed Databases: Distributed Data Storage: Fragmentation and Replication, Location and Fragment Transparency, Distributed Query Processing and Optimization, Distributed Transaction Modeling and Concurrency Control, Distributed Deadlock, Commit Protocols, Design of Parallel Databases, Parallel Query Evaluation. Advanced Transaction Processing: Nested and Multilevel Transactions, Compensating Transactions and Saga, Long Duration Transactions, Weak Levels of Consistency, Transaction Work Flows, Transaction Processing Monitors. Active Databases: Triggers in SQL, Event Constraint and Action: ECA Rules, Query Processing and Concurrency Control, Compensation and Databases Recovery. Real Time Databases: Temporal Constraints: Soft and Hard Constraints, Transaction Scheduling and Concurrency Control. Image and Multimedia Databases: Modeling and Storage of Image and Multimedia Data, Data Structures - R-tree, k-d tree, Q uadtrees, Content Based Retrival: Color Histograms, Textures etc, Image Features, Spatial and Topological Relationships, Multimedia Data Formats, Video Data Model, Audio and Handwritten Data, Geographic Information Systems (GIS). WEB Databases: Accessing Databases through WEB, WEB Servers, XML Databases, Commercial Systems: Oracle xxi, DB2. Data Mining: Knowledge Representation Using Rules, Association and Classification Rules, Sequential Patterns, Algorithms for Rule Accessing.

CS 60033 Logic Programming L-T-P: 3-0-0, Credit: 3

Propositional logic, First Order Logic: syntax and semantics, deduction, Herbrand interpretation and resolution methods, Syntax and Semantics of Logic Programs, Inference Rules, Unification and SLD-Resolution, Negation as Failure, Logic programming language PROLOG - a case study. Basic concepts, Recursive programming, Cuts and negation, Non-deterministic programming, Abstract computational model - Warren s Abstract Machine (WAM), Implementation of Prolog on WAM. Introduction to Constraint Logic Programming: Constraint logic programming scheme, Constraint satisfaction, constraint propagation, Constraint Logic Programming over the reals, Constraint Logic Programming over finite domains. Introduction to nonclassical logics. Modal logic. Accessibilty. Relation and Kripke possible world semantics. The logic of knowledge and belief, Autoepistemic knowledge, Temporal logic.

CS 60034 Advanced Microprocessor Based Systems L-T-P: 3-0-0, Credit: 3

Introduction: Basics of Von Neumann Architecture and the early Microprocessors, CISC and RISC concepts; Parallelism in Processor Architecture: Pipelining, Super-scalar, Super-pipeline and VLIW Architectures, Low-power Architecture; Built-in Multiprocessing support; Co-processors; Processor Architecture with hierarchical memory organization: Cache memory, Virtual memory; Built-in Multi-user and

multitasking support in 16-bit and 32 bit microprocessors, Built-in memory mapping and management support; Evolution of platform architecture; Special-purpose processor Architectures: Signal processing Microprocessors; Communication processors; Case studies with contemporary Microprocessors.

CS 60035 Information Retrieval **L-T-P: 3-0-0, Credit: 3**

Introduction: Principles of Information Retrieval, Indexing, Zipfs Law, Search. Vector space model, cosine similarity. Scoring techniques. Stemming, Stop words, Query expansion, Rochhio. Probabilistic models language. Relevance feedback. Evaluation: Precision, recall, f-measure. TREC Text classification, clustering, query routing. Advanced topics like summarization and question answering.

Suggested Text:

1. P Raghavan, M Manning and P Schutze, Introduction to Information Retrieval, Kluwer, 2007

CS 60036 Intelligent Systems **L-T-P: 3-0-0, Credit: 3**

Data, information and knowledge. Model of an intelligent system. Models of knowledge representations: Representation and reasoning in logic. Semantic representations: semantic networks, frames; Frame/script systems; Conceptual dependency and conceptual graphs. Ontologies. Knowledge based systems: Software architecture of a knowledge-based system, Rulebased programming and production systems, Rule chaining and inference control, Inference: reasoning about knowledge, Temporal reasoning, Inference under uncertainty: Bayesian techniques, Fuzzy reasoning, Casebased reasoning. Intelligent agents, The agent metaphor and attributes of agenthood, Agent theory and languages, Inter-agent communication, Ontological issues. Alternatives to the symbolic approach: Foundations of connectionist networks; their history. Applications of AI: Example application domains, e.g. Configuration, Diagnosis, Planning, intelligent interfaces, usermodelling, Practical implications of choosing and applying AI solutions. Knowledge representation and the Web, Semantic Web.

CS 60037 Embedded Systems **L-T-P: 3-1-0, Credit: 4**

Introduction to Embedded Systems - definitions and constraints; hardware and processor requirements; special purpose processors; input-output design and I/O communication protocols; design space exploration for constraint satisfaction; co-design approach; example system design; Formal approach to specification; specification languages; specification refinement and design; design validation; Real Time operating system issues with respect to embedded system applications; time constraints and performance analysis.

CS 60038 Advances in Operating Systems Design L-T-P: 3-0-0, Credit: 3

Theory and implementation aspects of distributed operating systems. Process synchronization in multiprocessing/multiprogramming systems. Inter-process communication and co-ordination in large distributed systems. Distributed resource management. Fundamentals of real time operating systems. Case studies. Information management in distributed systems: security, integrity and concurrency problems. Fault tolerance issues. OS issues related to the Internet, intranets, pervasive computing, embedded systems, mobile systems and wireless networks. Case studies of contemporary operating systems.

CS 60039 Testing and Verification of circuits L-T-P: 3-1-0, Credit: 4

Physical faults and their modeling. Fault equivalence and dominance; fault collapsing. Fault simulation: parallel, deductive and concurrent techniques; critical path tracing. Test generation for combinational circuits: Boolean difference, D-algorithm, Podem, etc. Exhaustive, random and weighted test pattern generation; aliasing and its effect on fault coverage. PLA testing: cross-point fault model, test generation, easily testable designs. Memory testing: permanent, intermittent and pattern-sensitive faults; test generation. Delay faults and hazards; test generation techniques. Test pattern generation for sequential circuits: ad-hoc and structures techniques, scan path and LSSD, boundary scan. Built-in self-test techniques. Verification: logic level (combinational and sequential circuits), RTL-level (data path and control path). Verification of embedded systems. Use of formal techniques: decision diagrams, logic-based approaches.

CS 60040 Parallel and Distributed Algorithms L-T-P: 3-0-0, Credit: 3

Fundamentals: Models of parallel and distributed computation, complexity measures; The PRAM Model: balancing, divide and conquer, parallel prefix computation, pointer jumping, symmetry breaking, list ranking, sorting and searching, graph algorithms, parallel complexity and complexity classes, lower bounds; Interconnection Networks: topologies (arrays and mesh networks, trees, systolic networks, hypercubes, butterfly) and fundamental algorithms, matrix algorithms, sorting, graph algorithms, routing, relationship with PRAM models; Asynchronous Parallel Computation; Distributed Algorithms: models and complexity measures, safety, liveness, termination, logical time and event ordering, global state and snapshot algorithms, mutual exclusion, clock synchronization, election, termination detection, routing, Distributed graph algorithms; Applications of Distributed algorithms.

CS 60041 Cryptography and Network Security L-T-P: 3-1-0, Credit: 4

Introduction: Basic objectives of cryptography, secret-key and public-key cryptography, one-way and trapdoor one-way functions, cryptanalysis, attack models, classical cryptography. Block ciphers: Modes of operation, DES and its variants, RCS, IDEA, SAFER, FEAL, BlowFish, AES, linear and differential cryptanalysis. Stream ciphers: Stream ciphers based on linear feedback shift registers, SEAL,

unconditional security. Message digest: Properties of hash functions, MD2, MD5 and SHA-1, keyed hash functions, attacks on hash functions. Public-key parameters: Modular arithmetic, gcd, primality testing, Chinese remainder theorem, modular square roots, finite fields. Intractable problems: Integer factorization problem, RSA problem, modular square root problem, discrete logarithm problem, Diffie-Hellman problem, known algorithms for solving the intractable problems. Public-key encryption: RSA, Rabin and EIGamal schemes, side channel attacks. Key exchange: Diffie-Hellman and MQV algorithms. Digital signatures: RSA, DAS and NR signature schemes, blind and undeniable signatures. Entity authentication: Passwords, challenge-response algorithms, zero-knowledge protocols. Standards: IEEE, RSA and ISO standards. Network issues: Certification, public-key infrastructure (PKI), secured socket layer (SSL), Kerberos. Advanced topics: Elliptic and hyper-elliptic curve cryptography, number field sieve, lattices and their applications in cryptography, hidden monomial cryptosystems, cryptographically secure random number generators.

CS 60042 Advances in Compiler Construction L-T-P: 3-1-0, Credit: 4

Review of compiler fundamentals - lexical analysis, parsing, semantic analysis, error recovery and intermediate code generation; Runtime storage management; Code generation; Code improvement - peephole optimization, dependence analysis and redundancy elimination, loop optimization, procedural and inter-procedural optimization, instruction scheduling, optimization for memory hierarchy; Compilation for high performance architecture; Portability and retargetability; Selected topics from compilers for imperative, object-oriented and mark-up languages, parallel and distributed programming and concurrency.

CS 60043 Algorithms for Bioinformatics L-T-P: 3-0-0, Credit: 3

Sequence similarity, homology, and alignment. Pairwise alignment: scoring model, dynamic programming algorithms, heuristic alignment, and pairwise alignment using Hidden Markov Models. Multiple alignment: scoring model, local alignment gapped and ungapped global alignment. Motif finding: motif models, finding occurrence of known sites, discovering new sites. Gene Finding: predicting reading frames, maximal dependence decomposition. Analysis of DNA microarray data using hierarchical clustering, model-based clustering, expectation-maximization clustering, Bayesian model selection.

CS 60044 Performance Evaluation and Reliability of Information Systems L-T-P: 3-0-0, Credit: 3

Review of probability and statistics, stochastic processes, Markov Models, Parameter estimation and hypothesis testing. Models of information systems, introduction to reliability measures. Estimation of MTF and other reliability parameters. Software metrics and software reliability models. Queuing network models, Workload design, Benchmarks, Estimations of performance metrics, case studies.

CS 60045 Artificial Intelligence **L-T-P: 3-0-0, Credit: 3**

Problem solving by search: state space, problem reduction, game playing, constraint satisfaction; Automated Reasoning: proposition and first order logic, inference and deduction, resolution refutation, answer extraction, knowledge based systems, logic programming and constrained logic programming, non-monotonic reasoning; Planning: state-space, plan space and partial order planning, planning algorithms; Reasoning under Uncertainty: probabilistic reasoning, belief networks; Learning: inductive learning, decision trees, logical approaches, computational learning theory, Neural networks, reinforcement learning; Intelligent Agents; Natural Language Understanding; Applications.

CS 60046 Real Time Systems **L-T-P: 3-0-0, Credit: 3**

Introduction to real time system, embedded systems and reactive systems; Hard and Soft Real Time Systems; Handling real time; Specification and Modeling; Design methods; Real Time operating systems; Validation and Verification; Real time Process and Applications; Distributed Real Time Systems.

CS 60047 Advanced Graph Theory **L-T-P: 3-1-0, Credit: 4**

Basic Concepts: Graphs and digraphs, incidence and adjacency matrices, isomorphism, the automorphism group; Trees: Equivalent definitions of trees and forests, Cayley's formula, the Matrix-Tree theorem, minimum spanning trees; Connectivity: Cut vertices, cut edges, bonds, the cycle space and the bond space, blocks, Menger s theorem; Paths and Cycles: Euler tours, Hamilton paths and cycles, theorems of Dirac, Ore, Bondy and Chvatal, girth, circumference, the Chinese Postman Problem, the Travelling Salesman problem, diameter and maximum degree, shortest paths; Matchings: Berge's Theorem, perfect matchings, Hall's theorem, Tutte's theorem, Konig's theorem, Petersen's theorem, algorithms for matching and weighted matching (in both bipartitie and general graphs), factors of graphs (decompositions of the complete graph), Tutte's f-factor theorem; Extremal problems: Independent sets and covering numbers, Turan's theorem, Ramsey theorems; Colorings: Brooks theorem, the greedy algorithm, the Welsh-Powell bound, critical graphs, chromatic polynomials, girth and chromatic number, Vizing's theorem; Graphs on surfaces: Planar graphs, duality, Euler's formula, Kuratowski's theorem, toroidal graphs, 2-cell embeddings, graphs on other surfaces; Directed graphs: Tournaments, directed paths and cycles, connectivity and strongly connected digraphs, branchings; Networks and flows: Flow cuts, Max flow min cut theorems, perfect square; Selected topics: Dominating sets, the reconstruction problem, intersection graphs, perfect graphs, random graphs.

CS 60048 Theory of Programming Languages **L-T-P: 3-0-0, Credit: 3**

Syntax of Programming Languages, Formal Language and Automata Theory: Finite Automata, Regular Languages, Pushdown Automata, Context Free Languages, Linear

Bounded Automata, Context Sensitive Languages, Turing machines and Recursively Enumerable Sets. Theory of LR(k) Parsing, Attribute Grammars. Semantics of Programming Languages: Basic Mathematical Introduction: Propositional and Predicate Calculus, Lambda Calculus, Algebraic Structures. Sequential Languages (Imperative and Applicative): Operational Semantics, Vienna Definition Methods, Denotational Semantics: Scott-Strachy Theory, Axiomatic Semantics: Floyd- Hoare Approach, Temporal Logic, Algebraic Semantics and Data Types.

CS 60049 Computational Complexity **L-T-P: 3-1-0, Credit: 4**

Models of Computation, resources (time and space), algorithms, computability, complexity; Complexity classes, P/NP/PSPACE, reductions, hardness, completeness, hierarchy, relationships between complexity classes; Randomized computation and complexity; Logical characterizations, incompleteness; Approximability; Circuit complexity, lower bounds; Parallel computation and complexity; Counting problems; Interactive proofs; Probabilistically checkable proofs; Communication complexity; Quantum computation.

CS 60050 Machine Learning **L-T-P: 3-0-0, Credit: 3**

The concept learning task. General-to-specific ordering of hypotheses. Version spaces. Inductive bias. Decision Tree Learning. Rule Learning: Propositional and First-Order, Over-fitting, Cross-Validation. Experimental Evaluation of Learning Algorithms Instance-Based Learning: k-Nearestneighbor algorithm, Radial basis functions. Case-based learning. Computational Learning Theory: probably approximately correct (PAC) learning. Sample complexity. Computational complexity of training. Vapnik-Chervonenkis dimension. Artificial Neural Networks : Linear threshold units, Perceptrons, Multilayer networks and backpropagation, recurrent networks. Probabilistic Machine Learning Maximum Likelihood Estimation, MAP, Bayes Classifiers Naive Bayes. Bayes optimal classifers. Minimum description length principle. Bayesian Networks, Inference in Bayesian Networks, Bayes Net Structure Learning Unlabelled data: EM, preventing overfitting, cotraining Gaussian Mixture Models, K-means and Hierarchical Clustering, Clustering and Unsupervised Learning, Hidden Markov Models, Reinforcement Learning Support Vector Machines Ensemble learning: boosting, bagging.

CS 60051 Discrete Structures **L-T-P: 3-1-0, Credit: 4**

Propositional Logic, Proof Methods of Implications, Sets, Basic operations on sets, Functions, Relations, Binary relations: Equivalence Relations, Partial Orders and Posets. Mathematical Induction, Pigeonhole Principle, First Order Logic and Other Proof Methods. Cardinality of sets, Finite and Infinite Sets, Countable and Uncountable Sets, Cantor's Theorem. Algebraic Structures: Semigroups, Monoids, Groups, Substructures and Morphisms, Rings, Fields and Vector Spaces; Lattices,

Boolean Algebras, Morphisms of Boolean Algebras; Basic Counting Principles, Permutations, Combinations, Recurrence Relations and their solutions.

CS 60052 Advanced Digital Image Processing and Computer Vision **L-T-P: 3-0-0, Credit: 3**

Sensor and Imaging: Imaging Optics, Radiometry of Imaging, Illumination sources and techniques, Camera Principles, Color Imaging, Single Sensor Color Imaging and Color Demosaicing, Range Images, 3D Imaging. Signal Representation: Vector Space and Unitary Trasnsforms, Multi-Resolutional Signal Representation, Wavelet Decomposition, Scale space and diffusion, Representation of color, Retinex Processing, Markov Random Field Modellings of Images. Non-linear Image Processing: Median and Order Statistics Filters, Rank-Ordered-Mean Filters and Signal Dependent Rank-Ordered-Mean Filters, Two Dimensional Teager Filters, Applications of nonlinear filters in image enhancement, edge detections, noise removal etc. Feature Estimation: Morphological Operations, Edge Detection, Edges in multichannel images, Texture Analysis, Optical flow based motion estimation, Reflectance based shape recovery, Depth from focus, Stereo matching and depth estimation. Image and Video Compression Standards: Lossy and lossless compression schemes: Transform Based, Sub-band Decomposition, Entropy Encoding, JPEG, JPEG2000, MPEG-1, MPEG-4, and MPEG-7. Object Analysis, Classification: Bayesian Classification, Fuzzy Classification, Neural Network Classifiers, Shape Reconstruction from volumetric data, Knowledge-based interpretation of images.

CS 60053 VLSI System Design **L-T-P: 3-1-0, Credit: 4**

Introduction to VLSI Design, Different types of VLSI design styles: Full custom, standard cell based, gate array based, programmable logic, field programmable gate arrays etc. VLSI Design flow. CMOS logic: PMOS, NMOS and CMOS, Electrical characteristics, operation of MOS transistors as a switch and an amplifier, MOS inverter, stick diagram, design rules and layout, delay analysis, different type of MOS circuits: Dynamic logic, BiCMOS, pass transistors etc. CMOS process, Combinational logic cells, Sequential logic cells, Datapath logic cells, I/O cells. ASIC Library Design: Transistors as Resistors and parasitic Capacitance, Logical effort, gate array, standard cell and datapath cell design. Introduction to hardware description language (HDL) Verilog/VHDL. A logic synthesis example. Floor-planning and Placement: I/O and power planning, clock planning. Routing global and detailed. Example design technique: mapping of architecture to silicon.

CS 60054 Low Power Circuits Design **L-T-P: 3-0-0, Credit: 3**

Low-Power Design Methodologies: an Overview: Why Low-Power? Low- Voltage Device Modeling: Spice models for MOS transistor; CMOS low voltage analytical model; CMOS Power supply voltage scaling. Low-Power CMOS Circuit Design: CMOS inverter characteristics, delay and power estimation; Sources of Power dissipation; Parameters involved in power dissipation; Switching activity in CMOS circuits; Adiabatic switching concepts; Dynamic CMOS circuits, Pass-transistor circuits; Low-Power circuit techniques; Multi-threshold CMOS circuit design. Low-

Power BICMOS Circuit Design: Characteristics of BICMOS logic circuits; Low-voltage BICMOS families. Low-voltage BICMOS Applications. Low-power VLSI Design Methodologies: Low-Power Physical design; Low-power gate level design; Low-Power Architecture level design, Algorithmic-level Power Reduction, Power estimation techniques.

CS 60055 Ubiquitous Computing **L-T-P: 3-0-0, Credit: 3**

Overview of wireless technologies, Signal propagation, Multiplexing, Modulation, and Spread spectrum techniques. Media access control: FDMA, TDMA, CDMA. Cellular systems: AMPS, GSM, DECT, UMTS, IMT-2000. CDMA-based cellular systems. Satellite systems: basic routing, localization, and handoff issues. Wireless Networks: packet radio network, Wireless LAN:IEEE 802.11b, Blue-tooth, Wireless ATM. Wireless Application Protocol (WAP) and WML. Mobile Networking: Mobile IP, Ad-Hoc Networks: AODV, DSR, DSDV routing. Wireless TCP: indirect TCP, Snooping TCP, Mobile TCP. Information Management, Location-Independent and Locationdependent computing models, Mobile applications and services, Security.

CS 60056 Computer Graphics **L-T-P: 3-1-0, Credit: 4**

Introduction: Display of entities, Geometric computation and representation, Graphics Environments; Working Principles of display devices: refreshing raster scan devices, vector devices, Cathode Ray Tube Terminals, Plotters; Display of colors: Look Up Tables, display of gray shades, Half toning; Display and drawing of graphics primitives: point, line, polygon, circle, curves and text; Coordinate Conventions: world coordinates, device coordinates, normalized device coordinates, view-port and window, zooming and panning by changing coordinate reference frames; Computations on polygons: point inclusion problem, polygon filling, polygon intersection, clipping, polygonization of a point set, convex hull computation, triangulation of polygons; Transformations in 2D and 3D: translation, rotation, scaling, reflection, Projection: perspective and parallel projections, isometric projection, Transformation matrices; Volume and Surface Representation: polygonal meshes, parametric curves and surfaces, Cubic and Bicubic Splines, Voxel, Octree and Medial Axis representation, Sweep Representation, Surfaces and Volumes by rotation of curves and surfaces, fractal modeling; Hidden surface and line elimination: Elimination of back surfaces, painters' algorithms, Binary Space Partitioning Tree; Rendering and Visualization: Shading model, Constant, Goraud and Phong Shading, Ray tracing algorithm, Radiosity Computation; Computer Animation: fundamental concepts.

CS 60057 Speech and Natural Language Processing **L-T-P: 3-0-0, Credit: 3**

Speech and Natural Language Processing: Introduction; Brief Review of Regular Expressions and Automata; Finite State Transducers; Word level Morphology and Computational Phonology; Basic Text to Speech; Introduction to HMMs and Speech Recognition. Indian language case studies; Part of Speech Tagging; Parsing with

CFGs; Probabilistic Parsing. Representation of Meaning; Semantic Analysis; Lexical Semantics; Word Sense; Disambiguation; Discourse understanding; Natural Language Generation; Techniques of Machine Translation; Indian Language case studies.

CS 60058 Fault Tolerant Systems **L-T-P: 3-0-0, Credit: 3**

Fundamental concepts in the theory of reliable computer systems design. Introduction to redundancy theory, limit theorems; decision theory in redundant systems. Hardware fault tolerance, redundancy techniques, detection of faults, replication and compression techniques, self-repairing techniques, concentrated and distributed voters, models of fault tolerant computing systems. Case studies. Software fault tolerance: fault tolerance versus fault intolerance, errors and their management strategies. Implementation techniques: software defense, protective redundancy, architectural support. Fault recovery techniques. Coding theory: application to fault tolerant system design. Fault-tolerance and reliability of multicomputer networks (direct and indirect) including fault-tolerant routing and sparing techniques. Yield and reliability enhancement techniques for VLSI/WSI array processors.

CS 60059 Object Oriented Systems **L-T-P: 3-0-0, Credit: 3**

Review of programming practices and code-reuse; Object model and object-oriented concepts; Object-oriented programming languages and implementation; Object-oriented analyses and design using UML structural, behavioral and architectural modeling; Unified development process, Software reuse design patterns, components and framework; Distributed object computing, interoperability and middleware standards COM/DCOM and CORBA; Object-oriented database system data model, object definition and query language, object-relational system.

CS 60060 Formal Systems **L-T-P: 3-1-0, Credit: 4**

Formal languages and their related automata, Turing machines, type-0 languages, linear bounded automata and CSLs. Time and tape bounded Turing machines, time and space bounds for recognizing CFLs. Turing Computability: number theoretic computations by Turing machines and indexing. Axiomatic systems, their soundness and completeness. Recursive function theory: primitive recursive functions and primitive recursive predicates. Ackermann's function, recursive and general recursive functions. Computability and decidability: computable functions, computable sets, decision problems. Fixpoint theory of programs, functions and functionals, verification methods, Lambda calculus and applications.

CS 60062 Multimedia Systems **L-T-P: 3-0-0, Credit: 3**

An overview of multimedia system and media streams; Source representation and compression techniques text, speech and audio, still image and video; Graphics and

animation; Multi-modal communication; Multimedia communication, video conferencing, video-on-demand broadcasting issues, traffic shaping and networking support; Transcoding; Multimedia OS and middleware; Synchronization and QoS; Multimedia servers, databases and content management; Multimedia information system and applications.

CS 60064 Computational Geometry **L-T-P: 3-1-0, Credit: 4**

Convex hulls: construction in 2d and 3d, lower bounds; Triangulations: polygon triangulations, representations, point-set triangulations, planar graphs; Voronoi diagrams: construction and applications, variants; Delayney triangulations: divide-and-conquer, flip and incremental algorithms, duality of Voronoi diagrams, min-max angle properties; Geometric searching: pointlocation, fractional cascading, linear programming with prune and search, finger trees, concatenable queues, segment trees, interval trees; Visibility: algorithms for weak and strong visibility, visibility with reflections, art-gallery problems; Arrangements of lines: arrangements of hyperplanes, zone theorems, many-faces complexity and algorithms; Combinatorial geometry: Ham-sandwich cuts, Helly's theorems, k-sets, polytopes and hierarchies, polytopes and linear progarmming in d-dimensions, complexity of the union of convex sets, simply connected sets and visible regions; Sweep techniques: plane sweep for segment intersections, Fortune's sweep for Voronoi diagrams, topological sweep for line arrangements; Randomization in computational geometry: algorithms, techniques for counting; Robust geometric computing; Applications of computational geometry.

CS 60066 Software Engineering **L-T-P: 3-0-3, Credit: 5**

Introduction. Life cycle models, Requirements analysis and specification, Formal requirements specification. Fundamental issues in software design: goodness of design, cohesion, coupling. Function-oriented design: structured analysis and design. Overview of object-oriented concepts. Unified Modelling Language (UML). Unified design process. User interface design. Coding standards and guidelines. Code walkthrough and reviews. Unit testing. Black box and white box testing. Integration and system testing. Software quality and reliability. SEI CMM and ISO 9001. PSP and Six Sigma. Cleanroom technique. Software project management. Configuration management. Software maintenance issues and techniques. Software reuse. Client-server software development.

CS 60068 CAD for VLSI **L-T-P: 3-1-0, Credit: 4**

Introduction: VLSI design flow, challenges. Verilog/VHDL: introduction and use in synthesis, modeling combinational and sequential logic, writing test benches. Logic synthesis: two-level and multilevel gate-level optimization tools, state assignment of finite state machines. Basic concepts of high-level synthesis: partitioning, scheduling, allocation and binding. Technology mapping. Testability issues: fault modeling and

simulation, test generation, design for testability, built-in self-test. Testing SoC's. Basic concepts of verification. Physical design automation. Review of MOS/CMOS fabrication technology. VLSI design styles: full-custom, standard-cell, gate-array and FPGA. Physical design automation algorithms: floor-planning, placement, routing, compaction, design rule check, power and delay estimation, clock and power routing, etc. Special considerations for analog and mixed-signal designs.

CS 60070 Quantum Computing and Quantum Information Processing **L-T-P: 3-1-0, Credit: 4**

Mathematical foundations; quantum mechanical principles; quantum entanglement; reversible computation, qubits, quantum gates and registers; universal gates for quantum computing; quantum parallelism and simple quantum algorithms; quantum Fourier transforms and its applications, quantum search algorithms; elements of quantum automata and quantum complexity theory; introduction to quantum error correcting codes; entanglement assisted communication; elements of quantum information theory and quantum cryptography.

CS 60076 Advances in Digital & Mixed Signal Testing L-T-P: 3-0-0, Credit: 3

Delay fault testing: path delay test, transition faults, delay test methodologies. IDDQ testing: basic concept, faults detected, test generation, limitations, IDDQ design for testability. Functional testing of arithmetic and regular arrays. Functional testing of microprocessors and microcontrollers. Sequential circuit testing: time frame expansion and simulation-based approaches to ATPG, design of testable FSMs, use of coding theory. Advanced BIST techniques: theory of linear machines, practical BIST architectures. System-on-chip design and test: SOC testing problem, core-based design and system wrapper, proposed test architectures for SOC, platform-based design and testability issues.

DSP-based analog and mixed-signal test: functional DSP-based testing, static ADC and DAC testing methods, realizing emulated instruments, CODECD testing, future challenges. Model-based analog and mixed-signal test: analog fault models, levels of abstraction, analog fault simulation, analog ATPG. Analog test bus standard: analog circuit DFT, analog test bus, IEEE 1149.4 standard.

Main Text Books:

1. M.L. Bushnell and V.D. Agrawal, “Essentials of Electronic Testing”, Kluwer Academic Publishers, 2000.

2. A. Osseiran, “Analog and mixed-signal boundary scan: a guide to the IEEE 1149.4 test standard”, Kluwer Academic Publishers, 1999.

3. A. Krstic and K-T. Cheng, “Delay fault testing for VLSI circuits”, Kluwer Academic Publishers, 2003.

4. S. Chakravarty and P.J. Thadikaran, “Introduction to IDDQ testing”, Kluwer Academic Publishers, 1997.

CS 60078 Complex Networks L-T-P: 3-0-0, Credit: 3

Types of network: Social networks, Information networks, Technological networks, Biological networks.

Properties of network: Small world effect, transitivity and clustering, degree distribution, scale free networks, maximum degree; network resilience; mixing patterns; degree correlations; community structures; network navigation.

Random Graphs: Poisson random graphs, generalized random graphs, the configuration model, power-law degree distribution, directed graph, bipartite graph, degree correlations.

Models of network growth: Price's model, Barabasi and Albert's model, other growth models, vertex copying models.

Processes taking place on networks: Percolation theory and network resilience, Epidemiological processes.

Applications: Search on networks, exhaustive network search, guided network search, network navigation; network visualization.

References

1. S. N. Dorogovtsev and J. F. F. Mendes, Evolution of Networks, Oxford University Press.

2. Narsingh Deo, Graph Theory, Prentice Hall of India.

3. M. Newman, A-L Barabasi, D. J. Watts, The structure and dynamics of networks, Princeton University Press.

CS 60080 Selected Topics in Algorithms L-T-P: 3-1-0, Credit: 4

The objective of this course is to familiarize students with some contemporary research in the area of algorithm design and analysis. The treatment will be theoretical with emphasis on problem solving and will be primality assignments based.

- Models of computation and efficiency: Searching faster than O(log n), sorting faster than O(n log n).
- Randomized algorithms in graphs and geometry: The impact of using randomization for designing algorithms that are simpler and often more efficient than the deterministic counterparts for several fundamental problems like MST, mincuts, spanners, convex hulls, triangulations, etc. Typically analysis is often harder than design.
- Approximation algorithms: A set of rapidly evolving techniques that lead to provable approximation guarantees for hard optimization problems within polynomial running times. Unlike other communities dealing with the same problems the emphasis here is on provability of general instances and goes hand-in-hand with the "hardness of approximation" theory.

Each of the topics on their own could be easily a full semester course, so depending on the class response, we may pick and choose from the above list of topics.

CS60082 COMPUTATIONAL NUMBER THEORY L-T-P: 3-0-0, Credit: 3

Algorithms for integer arithmetic: Divisibility, gcd, modular arithmetic, modular exponentiation, Montgomery arithmetic, congruence, Chinese remainder theorem, Hensel lifting, orders and primitive roots, quadratic residues, integer and modular square roots, prime number theorem, continued fractions and rational approximations.

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

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

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

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

Integer factoring algorithms: Trial division, Pollard rho method, p-1 method, CFRAC method, quadratic sieve method, elliptic curve method.

Computing discrete logarithms over finite fields: Baby-step-giant-step method, Pollard rho method, Pohlig-Hellman method, index calculus methods, linear sieve method, Coppersmith's algorithm.

Applications: Algebraic coding theory, cryptography.

References

1. Victor Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press.
2. Maurice Mignotte, Mathematics for Computer Algebra, Springer-Verlag.
3. Ivan Niven, Herbert S. Zuckerman and H. L. Montgomery, An Introduction to the Theory of Numbers, John Wiley.
4. Joachim von zur Gathen and Juergen Gerhard, Modern Computer Algebra, Cambridge University Press.
5. Rudolf Lidl and Harald Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press.
6. Alfred J. Menezes, editor, Applications of Finite Fields, Kluwer Academic Publishers.
7. Joseph H. Silverman and John Tate, Rational Points on Elliptic Curves, Springer International Edition.
8. D. R. Hankerson, A. J. Menezes and S. A. Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag.

9. A. Das and C. E. Veni Madhavan, Public-key Cryptography: Theory and practice, Pearson Education Asia.
10. Henri Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag.

CS60084 FOUNDATIONS OF CRYPTOGRAPHY L-T-P: 3-1-0, Credit: 4

Introduction to Cryptography: Basics of Symmetric Key Cryptography, Basics of Assymetric Key Cryptography, Hardness of Functions

Notions of Semantic Security (SS) and Message Indistinguishability (MI): Proof of Equivalence of SS and MI, Hard Core Predicate, Trap-door permutation, Goldwasser-Micali Encryption

Goldreich-Levin Theorem: Relation between Hardcore Predicates and Trap-door permutations

Formal Notions of Attacks: Attacks under Message Indistinguishability: Chosen Plaintext Attack(IND-CPA), Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2), Attacks under Message Non-malleability: NM-CPA and NM-CCA2, Inter-relations among the attack model

Random Oracles: Provable Security and asymmetric cryptography, hash functions

One-way functions: Weak and Strong one way functions

Pseudo-random Generators (PRG): Blum-Micali-Yao Construction, Construction of more powerful PRG, Relation between One-way functions and PRG, Pseudo-random Functions (PRF)

Building a Pseudorandom Permutation: The Luby Rackoff Construction: Formal Definition, Application of the Luby Rackoff Construction to the construction of Block Ciphers, The DES in the light of Luby Rackoff Construction

Left or Right Security (LOR)

Message Authentication Codes (MACs): Formal Definition of Weak and Strong MACs, Using a PRF as a MAC, Variable length MAC

Public Key Signature Schemes: Formal Definitions, Signing and Verification, Formal Proofs of Security of Full Domain Hashing

Assumptions for Public Key Signature Schemes: One way functions Imply Secure One-time Signatures

Shamir's Secret Sharing Scheme

Formally Analyzing Cryptographic Protocols

Zero Knowledge Proofs and Protocols

References

1. Hans Delfs and Helmut Knebl, Introduction to Cryptography: Principles and Applications, Springer Verlag.
2. Wenbo Mao, Modern Cryptography, Theory and Practice, Pearson Education (Low Priced Edition)
3. Shaffi Goldwasser and Mihir Bellare, Lecture Notes on Cryptography, Available at http://citeseerx.ist.psu.edu/.
4. Oded Goldreich, Foundations of Cryptography, CRC Press (Low Priced Edition Available), Part 1 and Part 2

CS 69011 Computer Systems Lab-I L-T-P: 0-0-6, Credit: 4

Object-oriented programming concepts and implementation of abstract data types. Implementation of graph algorithms. Linear programming with applications. Basics of OS programming: process creation and synchronization, shared memory and semaphore, shell programming.

CS 69012 Computer Systems Lab-II L-T-P: 0-0-6, Credit: 4

Socket programming, database creation and update, building large client server applications. Basics of compiler writing using lex and yacc.

Information Technology CS63052 L-T-P: 3-0-3 Credit: 5

Prerequsites: None

Computers in clinical medicine and practice. Informatics and its relevance to medicine, cybernetics, virtual reality. Applications of Internet and world wide web in health care delivery, development and spread. Medical information storage and management patient medical history, records of physical and systematic examinations and investigations including laboratory, radiology, pathology, diagnosis and treatment. Introduction to medical knowledgebased systems. Interactive applications and multimedia medical information systems. Integrated hospital information systems. Computer aided learning and education for medical and para-medical professionals.