Προτεινόμενα θέματα για το μάθημα

Theoretical Computer Science II: Structural Complexity

Interactive Proof Systems: Introduction, Interactive Proofs (**IP**), Arthur-Merlin Games (**AM**): Private vs. Public coins, $\texttt{GNI} \in \mathbf{AM}[2]$ (Set Lower Bound protocol), $\mathbf{IP} = \mathbf{PSPACE}$ (Arithmetization Technique), Multi-Prover Protocols ($\mathbf{MIP} = \mathbf{NEXP}$), Zero-Knowledge and pseudorandom functions.

Probabilistically Checkable Proofs: Definitions, Gap & Constraint Satisfaction problems, low-degree testing, self-corrections of polynomials, PCP characterization of **NP** and **NEXP**, Overview of the proof, PCPs and Hardness of Approximations: Inapproximability results.

Natural Proofs: Definitions, main results and their significance.

Counting Complexity: Basic Classes: $\#\mathbf{P}$, $\oplus\mathbf{P}$, Valiant's & Toda's Theorems, Approximate Counting and Uniform Generation of Solutions.

Measure and Dimension in Complexity Classes Gales & Martingales, Resource-Bounded Measure, Measure Theory analogies, Kolmogorov's zero-one laws, Resource-bounded (Hausdorff) dimension, dimension characterization of complexity classes.

Decision Trees: Decision Tree Complexity, Certificate Complexity, Randomized Decision Trees, Topological & Algebraic Criteria.

Pseudorandomness: *Pseudorandom Constructions*: Pseudorandom Generators, Dispersers, Extractors, Expander Graphs, List-Decodable Codes etc.
-Expander Graphs: Combinatorial and algebraic definitions, random walks on expanders, explicit constructions, spectrum, error correcting codes and metric embedding using expanders.
-Applications to Complexity: Error reduction, Undirected Connectivity is in **L**, Dinur's proof of the **PCP** Theorem.
-Randomness Extractors: Definitions, min-entropy, explicit constructions and existence proofs.

Hardness Amplification: Average and worst case hardness of Boolean functions, Yao's XOR Lemma, Hardcore Predicates and One-Way Functions, Local & List Decoding, Hardness Amplification, Applications to uniform derandomization of Complexity Classes.

Derandomization of Complexity Classes: Basic introduction to the field, the nature of randomness in computation and mathematics, conjectures about its inherence.
Non-Uniform Derandomization: Hardness-Randomness tradeoffs (high-end & low-end), Pseudorandom Generators, The Nisan-Wigderson construction, Non-uniform results for **BPP** assuming circuit lower bounds & hard functions, other constructions of PRGs (using min-entropy and one-way functions), Derandomization vs. Lower Bounds.
Uniform Derandomization: Derandomization of **BPP** under uniform assumptions, Derandomization of **RP** and **AM** using easiness assumptions, gap-theorem interpretations, uniform hardness-randomness tradeoffs for **AM** and $\mathbf{AM} \cap co\mathbf{AM}$ (high-end & low-end).

Various Techniques and Notions in Structural Complexity Theory: Downward and Random self-reducibility, Bi-immunity, Mitoticity, sparse and tally sets, Density, Padding, Polynomial-time isomorphism, Infinity Often and Almost Everywhere Hierarchies, Hierarchies for semantic classes, Promise Problems, Reductions (Karp, Cook, 1-1, truth-table, query-monotonic) and relations among them, Arithmetization & Algebrization techniques, Tournament Divide & Conquer technique, Isolation technique, Witness Reduction technique, Random Restriction technique etc.

Algebraic Computation: Algebraic Circuits, the classes $\mathbf{AlgP}_{/\mathbf{poly}}$, $\mathbf{AlgNP}_{/\mathbf{poly}}$, Topological methods for lower bounds in algebraic computation trees, Complexity and Real Computation: Introduction to the Blum-Shub-Smale model.

Proof Complexity: Propositional Calculus and Resolution, lower bounds, interpolation theorems, various proof systems, foundational issues.

Communication Complexity: Two-party and multi-party communication complexity, lower bounds, communication models, main topics and results.

Parameterized Complexity: Introduction to the field, parameterized problems, fixed-parameter tractability, approximability, fixed-parameter tractable reductions, the classes $para\mathbf{NP}$, $\mathbf{XP}$ and $\mathbf{W}[\mathbf{P}]$, W-Hierarchy and A-Hierarchy.

Average-Case Complexity: Definitions, Probability ensembles, distributional problems, the classes $dist\mathbf{P}$, $dist\mathbf{NP}$ and $samp\mathbf{NP}$, average-case reductions, main results.