Προτεινόμενα θέματα για το μάθημα

Theoretical Computer Science II: Advanced Topics in Algorithms and Complexity

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

- *Προτεινόμενη Βιβλιογραφία:*
  1. [AB09] Arora-Barak textbook, Chapter 8
  2. [Gol08] Goldreich's textbook, Section 9.1
  3. [GS86] S. Goldwasser, M. Sipser, *Private coins versus public coins in interactive proof systems*
  4. [BM88] L. Babai, S. Moran, *Arthur-Merlin Games: A randomized proof system, and a hierarchy of complexity classes*
  5. [FGM$^+$89] M. Fürer, O. Goldreich, Y. Mansour, M. Sipser, and S. Zachos, *On completeness and soundness in interactive proof systems*
  6. [BHZ87] R. Boppana, J. Håstad, and S. Zachos, *Does co-NP have short interactive proofs?*
  7. [Sha92] A. Shamir, **IP** = **PSPACE**
  8. [BF91] L. Babai, L. Fortnow, *Arithmetization: A new method in structural complexity theory*

Natural Proofs: Definitions, main results and their significance.

- *Προτεινόμενη Βιβλιογραφία:*
  1. Arora-Barak textbook, Chapter 23
  2. A. Razborov, S. Rudich, *Natural Proofs*, 1997
  3. Eric Allender, *Crack in the defenses: Scouting out approaches on circuit lower bounds*, 2008

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

- *Προτεινόμενη Βιβλιογραφία:*
  1. Arora-Barak textbook, Chapter 17
  2. Goldreich's textbook, Section 6.2
  3. [For97] L. Fortnow, *Counting Complexity*
  4. [Tor90] J. Torán, *Counting the number of solutions*
  5. [JVV86] M. Jerrum, L. Valiant, and V. Vazirani, *Random generation of combinatorial structures from a uniform distribution*
  6. [SJ89] A. Sinclair and M. Jerrum, *Approximate counting, uniform generation and rapidly mixing markov chains*

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.

- *Προτεινόμενη Βιβλιογραφία:*

  1. J. Lutz, *Resource-Bounded Measure*, 2011
  2. [Mos08] P. Moser, *Resource-bounded measure on probabilistic classes*
  3. [GL08] X. Gu and J. Lutz, *Dimension characterizations of complexity classes*
  4. [HLM05] J.M. Hitchcock, J.H. Lutz, and E. Mayordomo, *The fractal geometry of complexity classes*
  5. [Lut92] Jack H. Lutz *Almost everywhere high nonuniform complexity*
  6. [Lut03] Jack H. Lutz, *Dimension in complexity classes*
  7. [VW97] H. Vollmer and K. Wagner, *Measure one results in computational complexity theory*

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

- *Προτεινόμενη Βιβλιογραφία:*

  1. Arora-Barak textbook, Chapter 12
  2. [DK00] Ding-Zhu Du and Ker-I Ko, *The Theory of Computational Complexity*, John Wiley & Sons, 2000
  3. H. Buhrman, R. de Wolf, *Complexity measures and decision tree complexity: a survey*

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.

- *Προτεινόμενη Βιβλιογραφία:*

  1. L. Trevisan: *Pseudorandomness and Combinatorial Constructions*
  2. R. Shaltiel: *Introduction to Randomness Extractors*
  3. [Vad07] S. Vadhan: *The unified theory of pseudorandomness* (Paper)
  4. S. Vadhan: *The unified theory of pseudorandomness* (Monography)
  5. S. Hoory, N. Linial, and A. Wigderson: *Expander Graphs and their application*, Bulletin of the American Mathematical Society
  6. O. Reinglod: *Undirected ST-connectivity in log-space*
  7. I. Dinur: *The PCP Theorem by gap amplification*
  8. J. Radhakrishnan and M. Sudan, *On Dinur's proof of the PCP Theorem*
  9. [AK01] V. Arvind, J. Köbler: *On Pseudorandomness and Resource-Bounded Measure*
  10. A. Wigderson: *Deterministic Extractors*, Lecture Notes
  11. O. Goldreich: *Pseudorandomness, Part I*, Lecture Notes
  12. L. Trevisan: *Pseudorandomness, Part II*, Lecture Notes
  13. Goldreich's textbook, Chapter 8 (PRGs)

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.

- *Προτεινόμενη Βιβλιογραφία:*

  1. Arora-Barak textbook, Chapter 19
  2. [Sud01] Madhu Sudan, *Coding theory: Tutorial and survey*

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).

- *Προτεινόμενη Βιβλιογραφία (3-11: Lecture Notes and Surveys, 12-22 :Most important papers):*

  1. Arora-Barak textbook, Chapter 20
  2. Goldreich's textbook, Section 8.3 (Derandomization)

  ---

  3. P. Miltersen, *Derandomizing Complexity Classes*
  4. A. Wigderson: *Derandomizing* **BPP**, Lecture Notes
  5. [Nis96] N. Nisan, *Extracting randomness: How and why (a survey)*
  6. [Kab02] V. Kabanets, *Derandomization: a brief overview*
  7. [BFP03] H. Buhrman, L. Fortnow, and A. Pavan, *Some results on Derandomization*
  8. [For01] L. Fortnow, *Comparing notions of full Derandomization*
  9. [Imp03] R. Impagliazzo, *Hardness as Randomness: A survey of universal Derandomization*
  10. [Imp06] R. Impagliazzo, *Can every randomized algorithm be derandomized?*
  11. [Sha10] R. Shaltiel, *Typically-correct derandomization*

  ---

  12. [NW94] N. Nisan, A. Wigderson, *Hardness vs Randomness*
  13. [ISW06] R. Impagliazzo, R. Shaltiel, and A. Wigderson, *Reducing the seed length in the Nisan-Wigderson Generator*
  14. [IW97] R. Impagliazzo and A.Wigderson, ***P=BPP** unless **E** has sub-exponential circuits: Derandomizing the XOR lemma*
  15. [Uma03] C. Umans, *Pseudo-random generators for all hardnesses*
  16. [HILL99] J. Håstad, R. Impagliazzo, L. Levin, and M. Luby, *A pseudorandom generator from any one-way function*
  17. [BFNW93]Babai, Fortnow, Nisan & Wigderson, ***BPP** has subexponential time simulations unless **EXPTIME** has publishable proofs*
  18. [IW01] R. Impagliazzo and A.Wigderson, *Randomness vs Time: Derandomization under a Uniform Assumption.*
  19. [Kab00]V. Kabanets, *Easiness assumptions and hardness tests: Trading time for zero error*
  20. [Lu00] Chi-Jen Lu, *Derandomizing Arthur-Merlin Games under Uniform Assumptions*
  21. [GSTS03] D. Gutfreund, R. Shaltiel, and A. Ta-Shma, *Uniform hardness versus randomness tradeoffs for Arthur-Merlin games*
  22. [SU09] R. Shaltiel and C. Umans, *Low-end uniform hardness versus randomness tradeoffs for AM*

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.

- *Προτεινόμενη Βιβλιογραφία:*

1. Hemaspaandra-Ogihara, *The Complexity Theory Companion*, Springer, 2002
2. [DK00] Ding-Zhu Du and Ker-I Ko, *The Theory of Computational Complexity*, John Wiley & Sons, 2000
3. [BW89] R. v. Book and O. Watanabe, *A view of structural complexity theory*
4. [BF91] L. Babai, L. Fortnow *Arithmetization: A new method in structural complexity theory*
5. [LLS75] R. Ladner, N. Lynch, and A. L. Selman, *A comparison of polynomial time reducibilities*, 1975
6. [Gol05] O. Goldreich, *On Promise Problems (a survey in memory of Shimon Even)*
7. S. Aaronson and A. Wigderson, *Algebrization: A new barrier in complexity theory*
8. E. Allender, R. Beigel, U. Hertrampf, S. Homer, *Almost-everywhere complexity hierarchies for nondeterministic time*
9. [FS07]L. Fortnow, R. Santhanam, *Time hierarchies: A survey*
10. [FST05] Lance Fortnow, Rahul Santhanam, and Luca Trevisan, *Hierarchies for semantic classes*

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.

- *Προτεινόμενη Βιβλιογραφία:*

1. Arora-Barak textbook, Chapter 16
2. L. Blum, M. Shub, S. Smale, *On a theory of computation and complexity over the real numbers: **NP**-completeness, recursive functions and universal machines*, AMS, 1989
3. L. Blum, F. Cucker, M. Shub, S.Smale, *Complexity and Real Computation*, Springer-Verlag, 1997
4. [Val79] L. G. Valiant, *Completeness classes in algebra*

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

- *Προτεινόμενη Βιβλιογραφία:*

1. Arora-Barak textbook, Chapter 15
2. J. Krajíček, *Bounded arithmetic, propositional logic and Complexity Theory*, Cambridge University Press, 1995

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

- *Προτεινόμενη Βιβλιογραφία:*

1. Arora-Barak textbook, Chapter 13
2. E. Kushilevitz, N. Nisan, *Communication Complexity*, Cambridge University Press, 1997

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

- *Προτεινόμενη Βιβλιογραφία:*

  1. J. Flum, M. Grohe, *Parameterized Complexity Theory*, Springer-Verlag, 2006

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

- *Προτεινόμενη Βιβλιογραφία:*

  1. Arora-Barak textbook, Chapter 18
  2. Goldreich's textbook, Section 10.2
  3. [Wan97] J. Wang, Average-case computational complexity theory
  4. A. Bogdanov, L. Trevisan, *Average-Case Complexity*

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 1 edition, April 2009.

[AK01] V. Arvind and Johannes Köbler. On pseudorandomness and resource-bounded measure. *Theor. Comput. Sci.*, 255:205–221, March 2001.

[BF91] László Babai and Lance Fortnow. Arithmetization: A new method in structural complexity theory. *Computational Complexity*, 1:41–66, 1991.

[BFNW93] László Babai, Lance Fortnow, Noam Nisan, and Avi Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Comput. Complex.*, 3(4):307–318, 1993.

[BFP03] Harry Buhrman, Lance Fortnow, and Aduri Pavan. Some results on Derandomization. In *STACS '03: Proceedings of the 20th Annual Symposium on Theoretical Aspects of Computer Science*, pages 212–222, London, UK, 2003. Springer-Verlag.

[BHZ87] R. B. Boppana, J. Hastad, and S. Zachos. Does co-NP have short interactive proofs? *Inf. Process. Lett.*, 25:127–132, May 1987.

[BM88] László Babai and Shlomo Moran. Arthur-Merlin Games: A randomized proof system, and a hierarchy of complexity classes. *J. Comput. Syst. Sci.*, 36(2):254–276, 1988.

[BW89] Ronald V. Book and Osamu Watanabe. A view of structural complexity theory. *Bulletin of the EATCS*, 39:122–138, 1989.

[DK00] Ding-Zhu Du and Ker-I Ko. *Theory of Computational Complexity*. Wiley-Interscience, January 2000.

[FGM+89] Martin Fürer, Oded Goldreich, Yishay Mansour, Michael Sipser, and Stathis Zachos. On completeness and soundness in interactive proof systems. *Advances in Computing Research: Randomness and Computation (S. Micali, editor), JAI Press, Greenwich, CT*, 5:25–32, 1989.

[For97] Lance Fortnow. Counting Complexity. In *Complexity Theory Retrospective II*, pages 81–107. Springer-Verlag, 1997.

[For01] Lance Fortnow. Comparing notions of full Derandomization. In *CCC '01: Proceedings of the 16th Annual Conference on Computational Complexity*, page 28, Washington, DC, USA, 2001. IEEE Computer Society.

[FS07] Lance Fortnow and Rahul Santhanam. Time hierarchies: A survey. *Electronic Colloquium on Computational Complexity (ECCC)*, 14(004), 2007.

[FST05] Lance Fortnow, Rahul Santhanam, and Luca Trevisan. Hierarchies for semantic classes. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, STOC '05, pages 348–355, New York, NY, USA, 2005. ACM.

[GL08] Xiaoyang Gu and Jack H. Lutz. Dimension characterizations of complexity classes. *Computational Complexity*, 17(4):459–474, 2008.

[Gol05] Oded Goldreich. On Promise Problems (a survey in memory of Shimon Even [1935-2004]). *Electronic Colloquium on Computational Complexity (ECCC)*, (018), 2005.

[Gol08] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, 1 edition, April 2008.

[GS86] S Goldwasser and M Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, STOC '86, pages 59–68, New York, NY, USA, 1986. ACM.

[GSTS03] Dan Gutfreund, Ronen Shaltiel, and Amnon Ta-Shma. Uniform hardness versus randomness tradeoffs for Arthur-Merlin games. *Comput. Complex.*, 12:85–130, September 2003.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[HLM05] J.M. Hitchcock, J.H. Lutz, and E. Mayordomo. The fractal geometry of complexity classes. *SIGACT News*, 36:24–38, 2005.

[Imp03] Russell Impagliazzo. Hardness as randomness: a survey of universal Derandomization. *CoRR*, cs.CC/0304040, 2003.

[Imp06] Russell Impagliazzo. Can every randomized algorithm be derandomized? In *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, STOC '06, pages 373–374, New York, NY, USA, 2006. ACM.

[ISW06] Russell Impagliazzo, Ronen Shaltiel, and Avi Wigderson. Reducing the seed length in the Nisan-Wigderson Generator. *Combinatorica*, 26:647–681, December 2006.

[IW97] Russell Impagliazzo and Avi Wigderson. $P=BPP$ unless E has sub-exponential circuits: Derandomizing the *XOR* lemma. In *In Proceedings of the 29th STOC*, pages 220–229. ACM Press, 1997.

[IW01] Russell Impagliazzo and Avi Wigderson. Randomness vs Time: Derandomization under a Uniform Assumption. *J. Comput. Syst. Sci.*, 63:672–688, December 2001.

[JVV86] Mark Jerrum, Leslie G. Valiant, and Vijay V. Vazirani. Random generation of combinatorial structures from a uniform distribution. *Theor. Comput. Sci.*, 43:169–188, 1986.

[Kab00] Valentine Kabanets. Easiness assumptions and hardness tests: Trading time for zero error. In *Proceedings of the 15th Annual IEEE Conference on Computational Complexity*, COCO '00, pages 150–, Washington, DC, USA, 2000. IEEE Computer Society.

[Kab02] Valentine Kabanets. Derandomization: a brief overview. *Bulletin of the EATCS*, 76:88–103, 2002.

[LLS75] R. Ladner, N. Lynch, and A. L. Selman. A comparison of polynomial time redicibilities. *Theoretical Computer Science*, 22:155–171, 1975.

[Lu00] Chi-Jen Lu. Derandomizing Arthur-Merlin Games under Uniform Assumptions. *Computational Complexity*, 10:247–259, 2000.

[Lut92] Jack H. Lutz. Almost everywhere high nonuniform complexity. *J. Comput. Syst. Sci.*, 44(2):220–258, 1992.

[Lut03] Jack H. Lutz. Dimension in complexity classes. *SIAM Journal on Computing*, 32(5):1236–1259, 2003.

[Mos08] Philippe Moser. Resource-bounded measure on probabilistic classes. *Inf. Process. Lett.*, 106(6):241–245, 2008.

[Nis96] Noam Nisan. Extracting randomness: How and why (a survey). In *IEEE Conference on Computational Complexity*, pages 44–58, 1996.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs Randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, 1994.

[Sha92] Adi Shamir. IP = PSPACE. *J. ACM*, 39:869–877, October 1992.

[Sha10] Ronen Shaltiel. Typically-correct derandomization. *SIGACT News*, 41(2):57–72, 2010.

[SJ89] Alistair Sinclair and Mark Jerrum. Approximate counting, uniform generation and rapidly mixing markov chains. *Inf. Comput.*, 82(1):93–133, 1989.

[SU09] Ronen Shaltiel and Christopher Umans. Low-end uniform hardness versus randomness tradeoffs for AM. *SIAM J. Comput.*, 39(3):1006–1037, 2009.

[Sud01] Madhu Sudan. Coding theory: Tutorial and survey. In *FOCS*, pages 36–53, 2001.

[Tor90] Jacobo Torán. Counting the number of solutions. In Branislav Rovan, editor, *Mathematical Foundations of Computer Science 1990, MFCS'90, Banská Bystrica, Czechoslovakia, August 27-31, 1990, Proceedings*, volume 452 of *Lecture Notes in Computer Science*, pages 121–134. Springer, 1990.

[Uma03] Christopher Umans. Pseudo-random generators for all hardness. *Journal of Computer and System Science*, pages 419–440, 2003.

[Vad07] S. Vadhan. The unified theory of pseudorandomness: guest column. *SIGACT News*, 38:39–54, September 2007.

[Val79] Leslie G. Valiant. The complexity of enumeration and reliability problems. *SIAM J. Comput.*, 8(3):410–421, 1979.

[VW97] Heribert Vollmer and Klaus W. Wagner. Measure one results in computational complexity theory. In *Advances in Algorithms, Languages, and Complexity*, pages 285–312, 1997.

[Wan97] Jie Wang. *Average-case computational complexity theory*, pages 295–328. Springer-Verlag New York, Inc., New York, NY, USA, 1997.