Syllabus of "Computaional Complexity 2023/2024"

Massimo Lauria

December 15, 2023

`https://www.massimolauria.net/complexity2023/journal.html`

1 Bibliography

The main textbook of the course is

- [AB] Arora, Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2007.

Additional material on communication complexity and proof complexity are in

- [J] Jukna. *Boolean Function Complexity*. Springer, 2012.
- [RY] Rao, Yehudayoff. *Communication Complexity and Applications*. Cambridge University Press, 2020.

A proof from the last part of the course is only published, as far as I know, in

- [K] Knuth, the Art of Computer Programming Vol.4B [Page 238/239]

All reference to a textbook refer to book [AB] unless specified otherwise.

2 Introduction

- Introduction
- Chapter 0
- Parity on n variables requires CNF formulas of size $\Theta(n2^n)$
- Equality of two strings of n bits requires n bits of communication

3 Turing machines, Universality, Uncomputability, the class P

- Sections 1.1, 1.2, 1.3, 1.4
- Sections 1.5, 1.6
- Exercises 1.2, 1.3, 1.5, 1.8, 1.14
- Read and ponder the statement of Exercise 1.6, 1.7 and 1.9

4 NP and NP-completeness

- Karp reductions
- NP-completeness
- Non deterministic Turing Machines
- Cook-Levin theorem proved via Circuit-SAT (see Section 6.1 and Theorem 6.6)
- Decision vs Seach
- coNP, EXP, NEXP
- Implications of P vs NP
- Sections 2.1, 2.2, 2.3 (Section 2.3.4 is optional), 2.4, 2.5, 2.6, 2.7
- Exercises 2.1, 2.2, 2.4, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.14, 2.15, 2.16, 2.17, 2.18, 2.21, 2.23, 2.24, 2.25, 2.26, 2.27, 2.29, 2.30, 2.31, 2.34.

Students presentation Problems and reductions presented by the students are part of the program. We saw the NP-completeness of the following problems.

- 3-coloring: reduction from 3-CNF SAT
- Subset Sum: reduction from Independent Set
- Hamiltonian Path: reduction from 3-SAT
- 0,1-Integer programming: reduction from 3-SAT
- Subgraph Isomorphism: reduction from k-Clique

5 Boolean circuits

- Section 6.1, 6.3, 6.5
- Read Exercise 6.1
- Prove that any boolean circuit of size S on n-variables can be converted to the DeMorgan format, so that the new circuit has size at most $2S$.
- Prove that any function $f : \{0,1\}^n \longrightarrow \{0,1\}$ can be computed by a CNF of size $O(n2^n)$.
- Prove that any function $f : \{0,1\}^n \longrightarrow \{0,1\}$ can be computed by a boolean circuit of size $O(2^n)$.
- Theorem 1.29 on Jukna's book [J]

6 Randomized computation, RP, coRP, BPP, ZPP

- Appendix A.2
- Sections 7.1, 7.2 (no 7.2.4), 7.3, 7.4, 7.5.1
- Exercises 7.1, 7.4, 7.5, 7.6

7 Space complexity, NL-completeness

- The Graph of configurations
- PSPACE, TQBF is PSPACE-complete
- Savitch's Theorem
- Lospace reductions and NL-completeness
- NL = coNL
- Sections 4.1 (no 4.1.3), 4.2, 4.3
- Exercises 4.1, 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11

8 Interactive Proofs and PSPACE

- randomness in interaction is necessary
- public vs private randomness
- IP, AM, MA classes
- protocol for Graph Non Isomorphism
- coNP $\in$ IP
- IP = PSPACE
- Sections 8.1, 8.2, 8.3
- Sections 8.2.2 and 8.2.3 are excluded from the program, but the statement of Theorems 8.12 and 8.13 are part of the program
- Exercises 8.1, 8.2, 8.6, 8.8

9 Decision trees

- decision trees
- worst case depth complexity
- certificate complexity
- just the statement that bs(f)<= 2 $(s(f))^4$ [Huang'19]
- Statement of Yao minimax Lemma
- Section 12
- Exercises 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7

10 Communication complexity

- A deterministic protocol induces partition in monocromatic combinatorial rectagles
- Methods of lower bound: fooling set, tiling, rank
- randomized communication complexity

- public vs private coins
- worst case vs average case (Minimax theorem)
- Sections 13.1, 13.2.1, 13.2.2, 13.2.3
- Exercises 13.1, 13.2, 13.5, 13.6, 13.9, 13.10, 13.16, 13.19
- discussion on why Exercise 13.3 seems wrong
- Chapter 1 up to page 15 included. [RY]
- Theorem 1.7, 1.9, 1.18 [RY]
- Chapter 3 [RY]: sections
  - "Some protocols" (equality, greater than)
  - "Randomized Communication complexity"
  - "Error reductions"
  - "Public to Private coins"
  - "Minimax" (without proof)

11 Proof complexity

- proof systems
- p-simulation
- resolution
- tree-like resolution == decision trees
- prover-delayer game for tree-like resolution [K]
- ordeding principle is hard for tree like resolution [K]
- ordering principle is easy for resolution
- pigeonhole principle is hard for resolution
- Cutting Planes simulates resolution
- Cutting Planes refutes PHP
- Section 15.1, 15.2.1

- Section 18.1, 18,4, 18.5 [J]
- Section 19.1, 19.2 [J]
- Exercises: weakening is not necessary in resolution refutations
- Exercises: in tree-like resolution we can avoid resolving on the same variable along any proof path.