SS 2012

Komplexitätstheorie

Ernst W. Mayr

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2012SS/kt/

Sommersemester 2012

Chapter 0 Organizational Matters

- Lectures:
  - 4SWS Tue 08:25–09:55 (MI HS2)
    Fri 08:25–09:55 (MI 00.13.009A)
    Compulsory elective in areas Algorithms and Scientific Computing, Informatics, Bioinformatics
    Module no. IN2007
- Exercises/Tutorial:
  - 2SWS Central exercise: Thu 12:30–14:00 (01.10.011)
  - Tutor: Chris Pinkau
- Valuation:
  - 4V+2ZÜ, 8 ECTS Points
- Office hours:
  - Fri 11:00–12:00 and by appointment

- Tutorials:
  - Chris Pinkau, MI 03.09.057 (pinkau@in.tum.de)
    Office hours: Wed 10:00–11:00
- Secretariat:
  - Mrs. Lissner, MI 03.09.052 (lissner@in.tum.de)

- Problem sets and final exam:
  - problem sets are made available on Tuesdays in class and/or on the course webpage
  - must be turned in a week later before class
  - are discussed in the tutorial
- Exam:
  - written exam, date: August 2, 2012, 08:15–11:30Uhr
  - the final exam is closed book, no auxiliary means are permitted except for one sheet of DIN-A4 paper, handwritten by yourself
  - probably 10 problem sets

- Prerequisites:
  - Grundlagen: Algorithmen und Datenstrukturen (GAD)
  - Diskrete Wahrscheinlichkeitstheorie (DWT)
  - Effiziente Algorithmen und Datenstrukturen
  - Randomisierte Algorithmen
- Supplementary courses:
  - Approximationsalgorithmen
  - Internetalgorithmik
  - Quantenalgorithmen
  - ...
- Webpage:

http://wwwmayr.in.tum.de/lehre/2012SS/kt/

1. Planned topics for the course

1. The computational model
2. $\mathcal{NP}$ and $\mathcal{NP}$-completeness
3. Diagonalization
4. Space complexity
5. The polynomial hierarchy and alternation
6. Boolean circuits
7. (Randomized computation)
8. Interactive proofs
9. Cryptography
10. ...

2. Literature


Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
Cambridge University Press: Cambridge-New York-Melbourne, 2009


Giorgio Ausiello, Pierluigi Creszenzi, Giorgio Gambosi, Viggo Kann, Alberto Marchetti-Spaccamela, Marco Protasi:
Complexity and approximation — Combinatorial optimization problems and their approximability properties,
Springer-Verlag: Berlin-Heidelberg, 1999


José L. Balcázar, Josep Díaz, Joaquim Gabarró:
Structural Complexity I (and II),
EATCS Monographs on Theoretical Computer Science, Springer-Verlag: Berlin-Heidelberg, 1995


Christos H. Papadimitriou:
Computational Complexity,
Addison-Wesley Publishing Company: London-Amsterdam-New York, 1994


Christos H. Papadimitriou, Kenneth Steiglitz:
Combinatorial optimization: Algorithms and complexity,
Prentice-Hall, Englewood Cliffs, NJ, 1982


Karl Rüdiger Reischuk:
Komplexitätstheorie — Band I: Grundlagen,
B.G. Teubner: Stuttgart-Leipzig, 1999


Michael Sipser:
Introduction to the Theory of Computation,
International Edition, Thomson Course Technology:
Australia-Canada-Mexico-Singapore-Spain-United Kingdom-United States, 2006

Ingo Wegener:
The coomplexity of Boolean functions,
Wiley-Teubner Series in Computer Science: Stuttgart-Chichester-New York, 1987,
http://eccc.hpi-web.de/static/books/The_Complexity_of_Boolean_Functions/

Further relevant research papers will be made available during the course.

3. Notational conventions

We use standard notation and basic concepts, as detailed e.g., in the introductory course on

Discrete Structures, IN0015

http://wwwmayr.in.tum.de/lehre/2011WS/ds/index.html.en

Chapter I The Computational Model

1. Some basic concepts

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 9–13, Cambridge University Press: Cambridge-New York-Melbourne, 2009

2. Turing machines

2.1 The model

2.2 Robustness

2.3 Gödel numbers and the Universal TM

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 13–23, Cambridge University Press: Cambridge-New York-Melbourne, 2009

2.4 Non-computable functions, the Halting Problem

2.5 Deterministic time and the class $\mathcal{P}$

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 23–29, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Chapter II $\mathcal{NP}$ and $\mathcal{NP}$-completeness

1. The class $\mathcal{NP}$

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 37–39, Cambridge University Press: Cambridge-New York-Melbourne, 2009

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 39–43, Cambridge University Press: Cambridge-New York-Melbourne, 2009

3.2 The Cook-Levin theorem

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 43–48, Cambridge University Press: Cambridge-New York-Melbourne, 2009

4. The web of reductions

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 48–53, Cambridge University Press: Cambridge-New York-Melbourne, 2009

5. Decision versus search

6. co$\mathcal{NP}$, EXP, and NEXP

7. Some implications

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 53–59, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Also see

Michael R. Garey, David S. Johnson:
Computers and Intractability: A Guide to the Theory of $\mathcal{NP}$-completeness,
W.H. Freeman and Company: New York-San Francisco, 1979

and the websites

A Compendium of NP Optimization Problems.

Complexity Zoo

7.1 $\mathcal{NP}$-complete problems cannot be sparse

See

Holenstein, Thomas
Complexity Theory,
p. 4–4, Script, ETH Zürich, 2010

Chapter III Diagonalization

1. Time and space hierarchy

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 63–64, Cambridge University Press: Cambridge-New York-Melbourne, 2009

2. Non-deterministic time hierarchy

3. Ladner's theorem

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 65–67, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Lance Fortnow, Bill Gasarch:
Computational Complexity Blog
Two Proofs of Ladner's Theorem, 2003

4. Oracle machines and limits of diagonalization

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 68–71, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Chapter IV Space Complexity

1. Configuration graphs

2. Some space complexity classes

3. PSPACE completeness

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 75–82, Cambridge University Press: Cambridge-New York-Melbourne, 2009

3.1 Savitch's theorem

3.2 PSPACE and strategies for game playing

4. $\mathcal{NL}$-completeness

4.1 Certificate definition of $\mathcal{NL}$: Read-once certificates

4.2 $\mathcal{NL} = \text{co}\mathcal{NL}$

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 82–88, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Further references:

Larry J. Stockmeyer, Albert R. Meyer:
Word problems requiring exponential time,
Proceedings of the 5th Symposium on Theory of Computing, p. 1–9 (1973)
This paper contains some important PSPACE-completeness results.

Albert R. Meyer, Larry J. Stockmeyer:
The equivalence problem for regular expressions with squaring requires exponential space,
Proceedings of the 13th Annual Symposium on Switching and Automata Theory, p. 125–129 (1972)
This paper contains an EXPSPACE-completeness result.

And here an $\mathcal{NL}$-machine based proof for $\mathcal{NL} = \text{co}\mathcal{NL}$:

Holenstein, Thomas
Complexity Theory,
p. 13–14, Script, ETH Zürich, 2010

Chapter V The Polynomial Hierarchy and Alternation

1. The class Σ_2^p

2. The polynomial hierarchy

3. Alternating Turing machines

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 91–96, Cambridge University Press: Cambridge-New York-Melbourne, 2009

4. Time versus alternations: Time-space tradeoffs for SAT

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 96–98, Cambridge University Press: Cambridge-New York-Melbourne, 2009

5. Defining the hierarchy via oracle machines

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 98–99, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Chapter VI Boolean Circuits

1. Boolean circuits and $\mathcal{P}_{/\mathrm{poly}}$

2. Uniformly generated circuits

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 101–105, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Leighton, F. Thomson:
Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes,
Morgan Kaufmann: San Mateo, 1992

3. Turing machines that take advice

4. $\mathcal{P}_{/\mathrm{poly}}$ and $\mathcal{NP}$

5. Circuit lower bounds

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 105–107, Cambridge University Press: Cambridge-New York-Melbourne, 2009

6. Non-uniform hierarchy theorem

7. Finer gradations among circuit classes

8. Circuits of exponential size

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 108–113, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Chapter VII Randomized Computation

1. Probabilistic Turing Machines

2. Some examples of PTMs

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 115–120, Cambridge University Press: Cambridge-New York-Melbourne, 2009

3. One-sided and zero-sided error: $\mathcal{RP}$, co$\mathcal{RP}$, ZPP

4. The robustness of our definitions

5. BPP $\subseteq \mathcal{P}_{/\mathrm{poly}}$

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 120–127, Cambridge University Press: Cambridge-New York-Melbourne, 2009

6. BPP is in $\mathcal{PH}$

7. Randomized reductions

8. Randomized space-bounded computation

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 127–132, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Chapter VIII Interactive Proofs

1. Interactive proofs: Some variations

1.1 Interactive proofs with deterministic verifier and prover

2. The class IP: Probabilistic verifier

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 147–150, Cambridge University Press: Cambridge-New York-Melbourne, 2009

3. Interactive proof for graph nonisomorphism

4. Public coins and AM

4.1 Simulating private coins

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 150–152, Cambridge University Press: Cambridge-New York-Melbourne, 2009

4.2 Set lower bound protocol

4.3 Some properties of $\mathcal{IP}$ and AM

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 152–156, Cambridge University Press: Cambridge-New York-Melbourne, 2009

4.4 Can GI be $\mathcal{NP}$-complete?

5. $\mathcal{IP}$ =PSPACE

5.1 Arithmetization

5.2 Interactive protocol for #SAT$_D$

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 157–159, Cambridge University Press: Cambridge-New York-Melbourne, 2009

5.3 Protocol for TQBF

See

Sanjeev Arora, Boaz Barak:
Computational Complexity — A Modern Approach,
p. 160–159, Cambridge University Press: Cambridge-New York-Melbourne, 2009

Holenstein, Thomas
Complexity Theory,
p. 64–69, Script, ETH Zürich, 2010