National Taiwan University
Department of Finance
and
Dept. Computer Science & Information Engineering
Yuh-Da而非

Notes
Theory of Computation Lecture
You may want to review discrete mathematics.

For last year’s lecture notes:


Check

— More “advanced” materials may be added.
— We more or less follow the topics of the book.
— The best book on the market for graduate students.

Papadimitriou, Computational Complexity. 2nd

Class Information
- Teaching assistants will be announced later.
- The best way for me to remember you in a large class is [a science concentrator] said that in his eighth semester of college, there was not a single science professor who could identify him by name. (New York Times, September 3, 2003)

- Please ask many questions in class.

More information and future lecture notes (in PostScript and PDF formats) can be found at www.csie.ntu.edu.tw/~lyuu/complexity.html
Missing the final examination will earn a "fail" grade.

- If you cannot make it to an examination, please email me beforehand (unless there is a legitimate reason).

- You must show up for the examinations in person.

- At least two examinations.

- Try some of the exercises at the end of each chapter.

- No homework.

- No roll calls.

Grading
Famous, master’s theses of the century.

Possibly the most important, and also the most complex. Shannon’s master’s thesis was also born. Shannon's thesis was design and analysis of switching circuits. Circuit

1938: Shannon (1916-2001) used Boolean algebra for the

machines.

1936: Turing defined Turing machines and oracle Turing

machines.

Church (1903-1995), Post (1921-1994), on computability.


incompleteness theorems and recursive functions.

1930-1931: Gödel’s (1906-1978) completeness and

A Brief History (Biais towards Complexity)
1959: Rabin and Scott's notion of nondeterminism.

1956: Ford and Fulkerson's network flows.

1949: Shannon's study of cryptography was published.

1949: Shannon established information theory.

1948: (Also Shannon (1948).)


1947: Dantzig invented linear programming simplex.

A Brief History (continued)
polynomial hierarchy.

1972–1973: Karp, Meyer, and Stockmeyer defined the

1972: Karp established the importance of NP-completeness.

1971: Cook invented the idea of NP-completeness.

By Karp in 1972.

1965: Edmonds identified NP and P (actual names were coined

Hiearchy theorems (see also Rabin (1960)).

1965: Hartmanis and Stearns started complexity theory and

Kolmogorov complexity (program size and randomness).

1964–1966: Solomonoff, Kolmogorov, and Chaitin formalized

A Brief History (continued)
public-key cryptography.

probabilistic algorithms (for primality testing).


1975: Ladner studied P-complete problems.

1973: Baker, Gill, and Solovay studied "P = NP relative to oracles."

1973: Meyer and Stockmeyer studied exponential time and

1973: Karp studied PSPACE-completeness.

A Brief History (continued)
1979: Yao founded communication complexity.

1979: Polynomial time.

1979: Khaitchyan proved that linear programming is in P.

1979: Pippenger defined NC.

1979: Valiant defined #P.

1979: Computational complexity.

1979: Carey and Johnson published their book on

1978: Fortune and Wyllie defined the PRAM model.

1978: Rivest, Shamir, and Adleman invented RSA.

1977: Gill formalized randomized complexity classes.

A Brief History (continued)
number generation on complexity theory.

1982–1984: Yao, Blum, and Micali founded pseudorandom
maximum flow problem is P-complete.

1982: Goldschlag, Shaw, and Staddon proved that the
1982: Yao founded secure multiparty computation.
1982: Goldwasser and Micali proposed probabilistic encryption.
levels.
1982: Shamir proposed cryptographically strong pseudorandom
agreement problems in distributed computing.
1980: Lamport, Shostak, and Pease defined the Byzantine
A Brief History (continued)
1985: Shraer and Tarjan invented on-line algorithms.

1985: Zero-knowledge proofs.

1985: Goldwasser, Micahli, and Rackoff invented monotone circuits.

1985: Razborov proved exponential lower bounds for monotone circuits.

1985: Razborov proved exponential lower bounds for parity circuits of constant depth.


1984: Valiant founded computational learning theory.

1983: Atri, Komlos, and Szemeredi constructed an $O(\log n)$-depth, $O(\log \log n)$-size sorting network.

A Brief History (continued)
on Steiner tree problems.

1990: Du and Hwang settled the Gillett-Pollak conjecture.

1990: Shamir proved IP=PSpace.

1989: Blum and Kannan proposed program checking.

equals cont.

1987-1988: Selberg and immersion proved that NL can be solved in randomized polynomial time.

1987: Adleman and Huang proved that primality testing complexity assumptions.

1986: Goldreich, Micali, and Wigderson proved that every problem in NP has a zero-knowledge proof under certain

A Brief History (continued)
A brief history (concluded)

A 2002: Agrawal, Kayal, and Saxena discovered a polynomial-time algorithm for primality testing.


1993: Bernstein, Vazirani, and Yao established quantum complexity theory.

1992: Arora, Lund, Motwani, Sudan, and Szegedy proved the PCP theorem.