Theory of Computation Lecture Notes

Yuh-Dauh Lyuu

Dept. Computer Science & Information Engineering

and

Department of Finance

National Taiwan University

Class Information

- Papadimitriou. *Computational Complexity*. 2nd printing. Addison-Wesley. 1995.
  - The best book on the market for graduate students.
  - We more or less follow the topics of the book.
  - More “advanced” materials may be added.
- Check

  `www.csie.ntu.edu.tw/~lyuu/complexity/2001`

  for last year’s lecture notes.
- You may want to review discrete mathematics.

Class Information (concluded)

- More information and future lecture notes (in PostScript and PDF formats) can be found at

  `www.csie.ntu.edu.tw/~lyuu/complexity.html`

- Please ask many questions in class.
  - That is perhaps the only way I can remember you in a large class.
- Teaching assistants will be announced later.

Grading

- No roll calls.
  - You do not have to show up for class.
- No homeworks.
  - Try some of the exercises at the end of each chapter.
- At least two examinations.
- You must show up for the examinations, in person.
- If you cannot make it to an examination, please email me beforehand (unless there is a legitimate reason).
- Missing the final examination will earn a "fail" grade.

A Brief History (Biased towards Complexity)

1930–1931: Gödel's (1906–1978) completeness and incompleteness theorems.

1935–1936: Kleene (1909–1994), Turing (1912–1954), Church (1903–1995), Post (1997–1954) on computability.

1936: Turing defined Turing machines and oracle Turing machines.

1938: Shannon (1916–2001) used boolean algebra for the design and analysis of switching circuits. Circuit complexity was also born. Shannon's master's thesis was "possibly the most important, and also the most famous, master's thesis of the century."

A Brief History (continued)

1947: Dantzig invented linear programming simplex algorithm.

1947: Paul Erdős (1913–1996) popularized the probabilistic method. (Also Shannon, 1948.)

1949: Shannon established information theory.

1949: Shannon's study of cryptography was published.

1956: Ford and Fulkerson's network flows.

1959: Rabin and Scott's notion of nondeterminism.

A Brief History (continued)

1964–1966: Solomonoff, Kolmogorov, and Chaitin formalized Kolmogorov complexity (program size and randomness).

1965: Hartmanis and Stearns started complexity theory and hierarchy theorems. (See also Rabin, 1960.)

1965: Edmonds identified NP and P (actual names were coined by Karp in 1972).

1971: Cook invented the idea of NP-completeness.

1972: Karp established the importance of NP-completeness.

1972–1973: Karp, Meyer, and Stockmeyer defined the polynomial hierarchy.

A Brief History (continued)

1973: Karp studied PSPACE-completeness.

1973: Meyer and Stockmeyer studied exponential time and space.

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

1975: Ladner studied P-completeness.

1976–1977: Rabin, Solovay, Strassen, and Miller proposed probabilistic algorithms (for primality testing).

1976–1978: Diffie, Hellman, and Merkle invented public-key cryptography.

A Brief History (continued)

1977: Gill formalized randomized complexity classes.

1978: Rivest, Shamir, and Adleman invented RSA.

1978: Fortune and Wyllie defined the PRAM model.

1979: Garey and Johnson published their book on computational complexity.

1979: Valiant defined #P.

1979: Pippenger defined NC.

1979: Khachiyan proved that linear programming is in polynomial time.

1979: Yao founded communication complexity.

A Brief History (continued)

1980: Lamport, Shostak, and Pease defined the Byzantine agreements problem in distributed computing.

1981: Shamir proposed cryptographically strong pseudorandom numbers.

1982: Goldwasser and Micali proposed probabilistic encryption.

1982: Yao founded secure multiparty computation.

1982: Goldschlager, Shaw, and Staples proved that the maximum flow problem is P-complete.

1982–1984: Yao, Blum, and Micali founded pseudorandom number generation on complexity theory.

A Brief History (continued)

1983: Ajtai, Komlós, and Szemerédi constructed an $O(\log n)$-depth, $O(n \log n)$-size sorting network.

1984: Valiant founded computational learning theory.

1984–1985: Furst, Saxe, Sipser, and Yao proved exponential bounds for parity circuits of constant depth.

1985: Razborov proved exponential lower bounds for monotone circuits.

1985: Goldwasser, Micali, and Rackoff invented zero-knowledge proofs.

1985: Sleator and Tarjan invented on-line algorithms.

A Brief History (continued)

1987: Adleman and Huang proved that primality testing can be solved in randomized polynomial time.

1987–1988: Szelepscényi and Immerman proved that NL equals coNL.

1989: Blum and Kannan proposed program checking.

1990: Shamir proved IP=PSPACE.

1990: Du and Hwang settled the Gilbert-Pollak conjecture on Steiner tree problems.

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

A Brief History (concluded)

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

1994: Shor presented a quantum polynomial-time algorithm for factoring.

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