

**Instructor**

*Name* Pankaj K. Agarwal  
*Office* D207 LSRC Bldg.  
*Phone* 660-6540  
*E-mail* pankaj@cs.duke.edu  
*URL* <http://www.cs.duke.edu/~pankaj>

**Prerequisite**

CPS 140 or equivalent.

**Grading Policy**

- Four Homeworks (approx.); weight 40%
- One midterm; weight 20%
- Final; weight 40%

**Text Book**

1. C.H. Papadimitriou, *Computational Complexity*, Addison Wesley, Reading, MA, 1993.

**Reference Books**

1. G. Ausiello, P. Crescenzi, G. Gambosi, V. Kann, A. Marchetti-Spaccamela, and M. Protasi, *Complexity and Approximation*, Springer, Heidelberg, 1999.
2. D.-Z. Du and K.-I Ko, *Theory of Computational Complexity*, Wiley Interscience, New York, 2000.
3. M. Garey and D. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman and Company, New York, 1979.
4. J. Hopcroft, R. Motwani, and J. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison Wesley, Reading, MA, 2001.

1. **Turing machines:** Basics, tape compression, linear speedup, nondeterministic turing machines, universal turning machines.
2. **Undecidability:** Halting problem, recursive and recursively enumerable languages, primitive recursive and recursive functions.
3. **Complexity measures:** Definitions, complexity measures, hierarchy theorems, gap theorem, relations among complexity measures, reachability methods.
4. **Reduction and completeness:** Reducibilities, complete problems, oracle turing machines.
5. **NP:** NP-Completeness, Cook's theorem, other NP-Complete problems, pseudo-polynomial time, co-NP,  $\text{co-NP} \cap \text{NP}$ , functional problems.
6. **Beyond NP:** #P, PSPACE, EXPTIME, EXPSPACE, relativized complexity, alternation, polynomial time hierarchy.
7. **Circuit complexity:** Boolean circuits, circuits and turing machines, uniform and nonuniform complexity, NC, P-completeness, monotone circuits.
8. **Randomized computation:** Randomized TM, randomized complexity classes, pseudorandomness, derandomization.
9. **Cryptography:** One-way functions, pseudo-random generators, protocols.
10. **Interactive proofs:** Proof systems, IP, arithmetization, proof systems for #SAT,  $\text{IP}=\text{PSPACE}$ , program testing.
11. **Approximability:** Approximation algorithms, approximation and complexity, nonapproximability, MAXSNP, PCP, PCP vs. NP.
12. **Other computing models:** Shub-Smale model, quantum computing, DNA computing.