CS 50010: Foundational Principles of Information Security: Module 1

Instructor: Benjamin Harsha

Office Hours: 1:00-2:00pm MTWR, or by appointment
Office: HAAS G60 - located in the small hallway branching off near G50

Course Website: cs.purdue.edu/homes/bharsha/cs50010.html

Note: Please note that this course may not be used on the Plan of Study for any CS graduate students other than those in the Information Security for Computing Professionals program.

Grading

Module 1 accounts for 50% of the grade for CS 50010. The grades for the module 1 section are distributed as follows:

55% - Module 1 Exam
20% - Projects
20% - Written assignments
5% - Participation

Projects

There will be 2 programming projects in this module, each worth 10% of the final module 1 grade. All projects must be turned in using the turnin system, which will be introduced in the description of project 1.

Project 1: Assigned Friday, June 16. Due 11:59pm Sunday, June 25

Project 2: Assigned Monday, June 26. Due 11:59pm Friday July 7

Projects are graded by running the submitted solution against test cases which are fed to the program via standard in. A description of the input file format and a few sample test cases will be provided with each project.

Projects may be completed in C, C++, or Java, according to your preference. When submitting you must make sure that your program compiles using the standard compilers available on Purdue's linux systems (i.e. gcc, g++, and javac).

Written Assignments

There will be 4 written assignments in this module, each worth 5% of the module grade. Each assignment will consist of several questions with written answers relating to the topics covered in the previous few lectures. Assignments may be handed in as a hard copy or emailed to the instructor by the start of lecture on the due date

Assignment 1: Logic, Sets, Asymptotics, Stacks and Queues
- Assigned: June 14
- Due: June 19, Start of lecture

Assignment 2: Recursion and Graphs
- Assigned: June 19
- Due: June 22, Start of lecture

Assignment 3: Trees, Search Trees, Heaps
- Assigned: June 22
- Due: June 28, Start of lecture

Assignment 4: Greedy Algorithms, Divide and Conquer, Complexity Classes
- Assigned: June 14
- Due: July 5, Start of lecture

Schedule

CS 50010 Module 1 will meet 4 times per week, Monday-Thursday 9:30-10:45am in LWSN 1106 (Right by the Cafe). Below is the planned schedule for the course, although small adjustments may occur along the way.

Week 1:

Lecture 1: Logic and Proofs

- Basic Logical Rule and Direct Proofs
- Contraposition and Contradiction
- Induction

Lecture 2: Sets and Limits

- Set notation and operations
- Limits
- Running time of programs

Lecture 3: Asymptotics

- Big Oh. some examples
- Big Omega and Big Theta, with examples
- Solving trickier asymptotic problems (multivariate, complex loops)

Lecture 4: Stacks, Queues, and Lists

- Linked Lists, operations & implementations
- Stacks using LL and Arrays, Array Doubling
- Queues using LL and Arrays, Project 1

Week 2:

Lecture 5: Recursion

- Recursion definition and examples (Fibonacci #s, Factorial, Binary Search)
- Recursive vs Iterative, when to use each approach
- How to show correctness (Using definitions, Recursion trees/stacks)

Lecture 6: Graphs and Trees

- Definition of Graphs and Trees, some examples
- Graph representations (Adj. matrix vs Edge List). Pros/cons
- Weighted and directed graphs

Lecture 7: Searching in Graphs and Trees

- Undirected Depth First Search
- Breadth First Search
- Applications (Random path generation, path finding, strongly connected components)

Lecture 8: Trees and Hashing

- Tree Traversals
- Hash functions, uses and applications

Hash tables

Week 3:

Lecture 9: Search trees
- Definition, several examples, operations
- Balanced Search Trees
- Search Trees vs Hash Tables

Lecture 10: Heaps
- Structure and operations
- Implementations
- Uses, Heapsort

Lecture 11: Greedy algorithms
- Definition, Selection sort
- interval selection, shortest path
- Minimum Spanning Trees

Lecture 12: Randomized Algorithms
- Definition
- Randomized selection, Las Vegas, Monte Carlo, examples
- Additional examples, bipartite matching, subset sum, primality testing

Week 4:

Lecture 13: Complexity classes
- P, NP, P vs NP
- NP-completeness, a few examples
- Pseudo-polynomial time

Lecture 14:
- Undecidability
- Definition, Halting Problem
- Review

Lecture 15: Exam 1
- 75 minutes
- Closed book closed notes
- One 3x5 notecard “cheat sheet”
- Style is short and long answer, similar to HW problems

Exam

The Module 1 exam is scheduled for July 5 at 9:30-10:45am in LWSN 1106. The exam will consist of both short and long written answer questions, similar in style to the questions given on the written assignments. You may bring one 3x5 notecard with some handwritten notes if you want.