CS 3233 Discrete Mathematical Structures – Fall 04

9/29/04

Material covered in class until 9/27/04

This is the material relevant for midterm 1

Week	Material
1	**Logic: logical formulas and quantifiers (Ch. 1.1 (until page 11 top), 1.2, 1.3 (until page 37), 1.4)** Propositions, logical operators ($\vee, \wedge, \neg, \rightarrow, \leftrightarrow$), truth tables. Implication $p \rightarrow q$ and its contrapositive $\neg q \rightarrow \neg p$. Logical equivalences. Quantifiers (existential and universal). Negation of logical formulas (deMorgan). Nested quantifiers.
2	**Proofs (Ch. 1.5 page 56 and pages 63–71)** Direct proof, indirect proof, proof by contradiction. Proof by cases, proof of equivalence ($\leftrightarrow$ is equivalent to $\rightarrow$ AND $\leftarrow$). Constructive and non-constructive existence proofs. Counterexamples to disprove a claim.
3	**Sets (Ch. 1.6, 1.7 (until page 91)) and Functions (Ch. 1.8)** Sets, operations on sets. Cartesian product. Power set. Set complement. Set identities (deMorgan's laws). $\cup$ corresponds to $\vee$, and $\cap$ corresponds to $\wedge$. Definition of a function. One-to-one, onto, bijection. Composition of functions $f \circ g$, inverse f^{-1}. Floor and ceiling.
4	**Algorithms and Complexity (Ch. 2.1 (until page 127); pictures on the web; Ch. 2.2, 2.3)** Algorithm description in 5 steps (1: Problem definition; input & output. 2: Informal description in words. 3: Pseudocode. 4: Proof of correctness. 5: Runtime analysis). Best case, worst case. Insertion sort. Binary search. big-Oh, $\Omega, Theta$. Analyse the runtime of an algorithm and give a big-Oh bound for it. Code snippets.
5	**Integers and Algorithms (Ch. 2.4, 2.5 (pages 175–179; pictures on the web)) and Cryptography (Ch. 2.6 (pages 191–194); RSA handout)** Division $a\|b$. Prime numbers, composite numbers. Congruences; mod and div. Greatest common divisor. Relatively prime. Fast modular exponentiation (compute $b^n \pmod m$ using repeated squaring and recursion). Euclidean algorithm. RSA: Definition (pick p, q and compute e, d), application (know how to code and decode), proof of correctness.
6	**Sequences and Summations (Ch. 3.2 (until page 233))** Sequences, arithmetic progression, geometric progression. Summations. Index substitution.

- Use the **pictures** on the web as an additional resource.
- A good review is to look over the **Key Terms and Results** at the end of every full chapter.
- The book provides many practice questions at the end of every section, as well as additional practice questions at the end of every full chapter. The answers to the odd numbered problems are given in the end of the book.

Midterm 1 is on Wednesday October 6 at the usual class time in the class room. It is closed-book and closed-notes.