CS250: Discrete Math for Computer Science

L34: Summary and Review

Rigorous introduction to discrete mathematics.

Structures and concepts central to computer science:

- logic,
- number theory,
- induction and recursion,
- graph theory,
- finite automata.

Main Goals: become fluent in the language of mathematics.

- **precise specifications**: **learn how to say exactly what you mean**
- **rigorous proofs**: **learn how to prove that what you say is correct**

- **PropCalc:** $\wedge, \vee, \sim, \rightarrow, \leftrightarrow$, truth tables, CNF, DNF
  English is ambiguous, Logic is precise, need to be able to translate back and forth.

- **PropCalc:** $\wedge, \vee, \sim, \rightarrow, \leftrightarrow$, truth tables, CNF, DNF
  English is ambiguous, Logic is precise, need to be able to translate back and forth.
- **PredCalc:** First-Order Logic with Equality, predicate symbols, function symbols, terms, atomic formulas, quantifiers, first-order formulas, free and bound variables, prenex normal form, logical structures and satisfiability, Tarski's Definition of Truth, Truth Game, Natural Deduction Proofs.

- **PropCalc:** $\wedge, \vee, \sim, \rightarrow, \leftrightarrow$, truth tables, CNF, DNF
  English is ambiguous, Logic is precise, need to be able to translate back and forth.
- **PredCalc:** First-Order Logic with Equality, predicate symbols, function symbols, terms, atomic formulas, quantifiers, first-order formulas, free and bound variables, prenex normal form, logical structures and satisfiability, Tarski's Definition of Truth, Truth Game, Natural Deduction Proofs.
- **Sets and functions:** domain, co-domain, range, 1:1, onto, composition, inverses, $\wp(S)$.

- **PropCalc:** $\wedge, \vee, \sim, \rightarrow, \leftrightarrow$, truth tables, CNF, DNF
  English is ambiguous, Logic is precise, need to be able to translate back and forth.
- **PredCalc:** First-Order Logic with Equality, predicate symbols, function symbols, terms, atomic formulas, quantifiers, first-order formulas, free and bound variables, prenex normal form, logical structures and satisfiability, Tarski's Definition of Truth, Truth Game, Natural Deduction Proofs.
- **Sets and functions:** domain, co-domain, range, 1:1, onto, composition, inverses, $\wp(S)$.
- **Induction:** for proving $\forall n\, \alpha(n)$, $n \in \mathbf{N}$, inductive definitions

- **Number Theory:** integers, divisibility, congruence and modular arithmetic, greatest common divisors, Euclid's algorithm, using Euclid's algorithm to compute multiplicative inverses mod m, Chinese Remainder Theorem, efficient exponentiation algorithm mod m with huge exponents, $\mathbf{Z}_m^\star$, Euler's φ function, Fermat's Little Thm, Euler's Thm, Cryptography and the RSA algorithm.

- **Number Theory:** integers, divisibility, congruence and modular arithmetic, greatest common divisors, Euclid's algorithm, using Euclid's algorithm to compute multiplicative inverses mod m, Chinese Remainder Theorem, efficient exponentiation algorithm mod m with huge exponents, $\mathbf{Z}_m^\star$, Euler's φ function, Fermat's Little Thm, Euler's Thm, Cryptography and the RSA algorithm.
- **Graphs:** directed and undirected, trees, cycles, walks and paths, connectivity of undirected graphs, strong connectivity of directed graphs, Eulerian walks, Euler's formula for undirected planar graphs, Depth First Search.

- **Number Theory:** integers, divisibility, congruence and modular arithmetic, greatest common divisors, Euclid's algorithm, using Euclid's algorithm to compute multiplicative inverses mod m, Chinese Remainder Theorem, efficient exponentiation algorithm mod m with huge exponents, $\mathbf{Z}_m^\star$, Euler's φ function, Fermat's Little Thm, Euler's Thm, Cryptography and the RSA algorithm.
- **Graphs:** directed and undirected, trees, cycles, walks and paths, connectivity of undirected graphs, strong connectivity of directed graphs, Eulerian walks, Euler's formula for undirected planar graphs, Depth First Search.
- **Regular Sets:** DFA, Regular Expressions, Pumping Lemma, NFA, ϵ transitions, Kleene's Thm.

Studying for the Final

1. Go over **solutions** to **homeworks**, **dicussions**, **quizzes** and **tests**.
2. Look over the **Lecture Slides**.
3. If you are challenged by a question on any of the above, **practice some similar problems**.
4. It wouldn't hurt to reread assigned sections of [Epp] and try any of her problems from those sections.
5. As you are studying, questions on **Piazza** about any of the above material are **welcome**.
6. Send me suggestions for the **final crib sheet** by this Friday.
7. Get a good night's sleep next Tuesday night.
8. At the final: **relax** and **work carefully**. The format will be similar to the first two tests and there will be plenty of time.