Midterm 2 Review

Sinho Chewi, Alvin Wan

CS70 Fall 2016

goo.gl/2lJr68

Review Format

- Divided into 8 sections, each ~22 minutes
- We want you to try problems
- For each section, we will run through the following:
  - I give tips (~2 minutes)
  - You do basic practice problem (~5 minutes)
  - I go over solutions (~2 minutes)
  - You do a more advanced practice problem (~10 minutes)
  - I go over solutions (~3 minutes)
- Goal: Learn approaches to classes of problems

Modular Arithmetic

Modular Arithmetic

- Related Concepts:
  - Divisibility
  - Euclid’s (Extended) Algorithm
  - Fermat’s Little Theorem
  - Chinese Remainder Theorem
  - Polynomials, Galois Fields

Bijections, RSA

Bijections, RSA

- Related Concepts
  - Public Key (N, e)
  - Private Key (d)
  - Encryption (x^e)
  - Decryption (x^d)

Polynomials

Polynomials

- Related Concepts
  - Roots, Factorization
  - Lagrange Interpolation
  - Secret Sharing

Errror Correcting

Error Correcting

- Related Concepts
  - Erasure Errors: Reed-Solomon
  - General Errors: Berlekamp-Welch

Infinity, Uncountability

Infinity, Uncountability

- Related Concepts
  - Countability: Bijections
  - Cantor’s Diagonalization Argument

Self-Reference, Uncomputability

Self-Reference, Uncomputability

- Related Concepts
  - Halting Problem
  - Reductions
  - Uncomputability

Counting

Counting

- Related Concepts
  - Addition Principle (Inclusion-Exclusion)
  - Multiplication Principle
  - Combinations/Permutations
  - Stars and Bars
  - Combinatorial Proofs

Probability

Probability

- Related Concepts
  - Probability Space (Ω), Axioms
  - Counting
  - Conditional Probability (Law of Total Probability)
  - Bayes Rule
  - Independence (Pairwise Independence, Mutual Independence)