Discrete Math (Spring 2019)

This is the official website of math314-02-s19.[1] Please read our syllabus...

Our Final Exam is scheduled for 13 May 2019.

Here are documents on basic proof techniques and proof-writing style for your own reference.

THIS PAGE NO LONGER RECEIVES UPDATES

General Information

Meetings: Monday, Wednesday, Friday 8am - 9:30am in WH G02

Office Hours: Tuesday 10am - 1pm in WH236 (or by appointment in WH310)

Textbook: Mathematics for Computer Science (Lehman, Leighton, Meyer)

Grading: See the course syllabus for a grade distribution.

Content: Propositional logic, methods of proof, naive set theory, functions and relations, induction and recursion, counting, and basic graph theory.

Schedule

W 23 Jan (C1)

- Discussed Syllabus
- Brief introduction to propositional logic (what is meant by the terms *statement*, *connective*, etc.)
- **HW**: Read textbook section 3.1 (4 pages)

F 25 Jan (C2)

- Translation of English statements into the formal language
- Truth tables (optional: read textbook section 3.2)
- **Practice**: problem set 1
- **HW**: Read textbook sections 3.3 and 3.4 (2 pages and 5 pages)

M 28 Jan (C3)

- Quiz: Truth table construction
- Validity, satisfiability, and logical equivalence
- Developed several basic equivalences of propositional statements.

W 30 Jan (C4)

- Disjunctive Normal Form and Conjunctive Normal Form
- Algebra of propositions (textbook section 3.4)
- Basic rules of equivalence
- **Practice**: problem set 2
- **HW**: Read textbook section 3.6 (5 pages)

F 1 Feb (C5)

- Quantified predicate logic (textbook section 3.6)

M 4 Feb (C6)

- Basics of sets (textbook section 4.1)
- Example proofs involving sets (direct proof)

W 6 Feb (C7)

- More proofs of set theoretic identities (proof by cases, proof via a string of equivalent statements).
- Introduced general relations (lots of examples)
- Defined equivalence relations
- **HW**: Read about functions and relations for Friday's class (caution: I'm NOT following the textbook here!)

F 8 Feb (C8)

- Equivalence relations (many examples)
- Introduction to functions (defined injective, surjective, and bijective)
- **Written Homework 1**: Complete this list of problems (Due 15 Feb 2019)

M 11 Feb (C9)

- Quiz: Equivalence relations
- Images and preimages, right and left inverses (many examples)
- Various propositions, examples, and practice problems concerning functions
- **HW**: Read textbook section 5.1 through section 5.1.4 (5 pages)

W 13 Feb (C10)

- Quiz: Functions and equivalence relations
- Relationship between functions inverses and injectivity, surjectivity, and bijectivity
- Introduction to the Principle of Mathematical Induction (textbook section 5.1.1-5.1.4)

F 15 Feb (C11)

- Collected Written Homework 1
- Quiz: Induction and Well Ordering
- More proofs by induction
- A false proof by induction (to illustrate the importance of the base case)!
- Number Theory: Properties of Divisibility (textbook section 9.1.1)

M 18 Feb (C12)

- Recursion and the relationship to induction
- Fibonacci numbers and relations therebetween (more induction proofs!)
- Here is a list of cool problems involving Fibonacci numbers!

W 20 Feb (C13)

- The Quotient-Remainder Theorem (i.e. the Division Algorithm, i.e. textbook Theorem 9.1.4 “The Division Theorem”)
- Proof of the Quotient-Remainder Theorem (for the case n and d are natural numbers)
- **HW**: Finish the proof of the Quotient-Remainder Theorem for n and d integers.

F 22 Feb (C14)

- Quiz: Quotient-Remainder Theorem
- Using the Quotient-Remainder Theorem
- Modular Arithmetic
- **HW**: Read my notes on basic number theory
- **Written Homework 2**: Complete this list of problems (Due 4 Mar 2019)

M 25 Feb (C15)

- Greatest common divisor
- Bezout's Identity (one proof given in this pdf)
- Euclid's (Extended) Algorithm
- Examples involving Euclid's Algorithm

W 27 Feb (C16)

- Quiz: Modular Arithmetic and Euclid's Algorithm
- Using Euclid's Algorithm to solve modular equations
- Prime numbers
  - Definition
  - Prop: Every natural number n > 1 is divisible by some prime number.
  - Prop: There are infinitely many prime numbers.

F 1 Mar (C17)

- Proved Euclid's Lemma
- Proved the Fundamental Theorem of Arithmetic via Strong Induction
  - **Exercise**: Translate the proof into a Well Ordering Principle type of proof
- Introduced the Sieve of Eratosthenes
- **NB**: I updated the number theory notes.

M 4 Mar (C18)

- Collected Written Homework 2.
- Computed the list of primes not exceeding 50 via the Seive of Eratosthenes.
- Briefly discussed some ways of improving the Seive of Eratosthenes.
- Discussed the RSA Cryptosystem (including a small example).
- **HW**: Read textbook section 9.11 (on RSA Cryptography)

W 6 Mar (C19)

- More work on RSA (try these problems).
- **HW** (assigned in class, sent also by email): Let p = 11, q = 19, and e = 13.
  - What is the corresponding public key?
  - Encrypt m = 19 using RSA encryption.
  - Compute the private key d in this encryption scheme.
  - Decrypt an encoded message m' = 47 using RSA.
- **Question**: Why does RSA work? (Answer: Euler's Totient Theorem!)
- Set the stage to study Euler's Totient Function

F 8 Mar (C20)

- Studied Euler's Totient Function, laying groundwork for the proof
- Proof of Correctness of RSA (assuming Euler's Totient Theorem)
- **HW**: Study for our Midterm Exam
  - Material for the Midterm stops at RSA
  - Know definitions and major theorems and be ready to use them
  - Be sure to look over your notes
  - By popular request, here is a practice midterm.
    - *Disclaimer*: The practice midterm DOES NOT pretend to be comprehensive, and I make no claims about its fitness as a study guide.

M 11 Mar (C21)

- Exam Review (questions from students)
- Proof of Euler's Totient Theorem
  - Remember that this implies correctness of the RSA Cryptosystem

NB: I leave for a visit to the IAS early Tuesday morning–I return after the midterm.

W 13 Mar (C22)

- Exam Review (led by guest lecturer David Cervantes Nava)
- Student questions on the Practice Exam
- Here are solutions to the practice midterm

F 15 Mar--Midterm Exam (in class)

- Happy Spring Break!
  - **HW**: Read textbook sections 15.1 - 15.3 on basic counting techniques

M 25 Mar (C23)

- Returned Midterm Exams
- Basics of counting
  - Addition Principle
  - Product Principle
  - Bijective Counting

W 27 Mar (C24)

- More counting (with many examples and some recursive counting)

F 29 Mar (C25)

- Problem session on basic counting techniques
  - Counting with binomial coefficients
- **HW**: Finish the in-class problems for Monday
- **HW**: Complete these problems for 5 Apr.

M 1 Apr (C26)

- More counting with binomial coefficients
  - Algebraic Formula for the binomial coefficients
  - Counting anagrams of a word
- Learned the methods “Count Dracula” and the method of Monte Cristo[2)]

T 2 Apr--Withdrawal Deadline

W 3 Apr (C27)

- Quiz: Binomial coefficients and counting
- More advanced counting techniques
  - Inclusion-Exclusion Principle
  - Pigeonhole Principle
- More counting!

F 5 Apr (C28)

- Quiz: Pigeonhole principle
- Collected Homework on counting poker hands
- Simple graphs (textbook chapter 12)
  - Basic definitions
  - Many examples (the Petersen graph is my favorite)
  - Handshake Lemma

M 8 Apr (C29)

- Quiz: examples of simple graphs
- Matchings in graphs
  - Examples
  - Basic results
  - Hall's Marriage Theorem for bipartite graphs
    - Statement
    - Proof of sufficiency

W 10 Apr (C30)

- Quiz: perfect matchings
- Hall's Marriage Theorem
  - Proof of necessity
- **Written Homework 3**: Complete this list of problems (due 26 Apr 2019)

F 12 Apr (C31)

- Quiz: Hall's Marriage Theorem
- Algorithms to compute matchings in bipartite graphs
  - Algorithm suggested by Hall's Marriage Theorem
  - Augmenting Paths Algorithm
- Connection in graphs

M 15 Apr (C32)

- Quiz: Augmenting Paths Algorithm
- Graph coloring
  - Many examples
  - Basic properties

W 17 Apr (C33)

- Quiz
- More graph coloring
  - Brooks's Theorem
    - Every finite simple graph has chromatic number bounded above by one more than its maximum degree.

F 19 Apr No Classes :/

M 22 Apr (C34)

- Group Quiz (discussion led by guest lecturer Kunle Abawonse)
  - Solutions to these problems

W 24 Apr (C35)

- Quiz: Graph coloring
- More on connection in graphs
  - Reducing problems on graphs to problems on their connected components
  - **Exercise**: Prove that the chromatic number of a graph is the maximum of the chromatic numbers of its components.
- Eulerian graphs (short introduction)

F 26 Apr (C36)

- Quiz: Euler trails
- Collected Homework 3
- Eulerian graphs
  - Proved Euler's characterization of Eulerian graphs
    - A graph has an Euler trail if and only if it has at most one component with edges and at most two vertices of odd degree.
- Hamiltonian graphs
  - No nice equivalent conditions are known
  - **Homework**: Does the Petersen graph have a Hamilton cycle?
    - Solution is in this pdf
- You should read about Leonhard Euler...

M 29 Apr (C37)

- Quiz
- Trees (Textbook section 12.11)
  - Equivalent descriptions of trees
  - Spanning trees
  - Minimum weight spanning trees
    - Kruskal's Algorithm

W 1 May (C38)

- Quiz: Kruskal's Algorithm
- Algorithms and state machines (Textbook chapter 6)
  - State machine definitions and examples
  - Evaluations
  - Preserved Invariant Lemma (Textbook “Preserved Invariant Principle”)
- Here are my notes on state machines.

F 3 May (C39)

- Quiz
- More algorithms and state machines
  - Examples encoding algorithms into state machines
  - Examples interpreting state machines as algorithms

M 6 May (C40)

- The fast exponentiation algorithm
  - State machine model
  - Proof of correctness

W 8 May (C41)

- Review for Final
  - Student questions
- Gave comment forms

F 10 May (C42)

- Review for Final
  - Student questions
- I will hold extra office hours today!
  - **Room**: WH 236
  - **Time**: 11am - 4pm

FINAL EXAM

- **Date**: Monday 13 May 2019
- **Time**: 8am - 10am
- **Room**: S1 149

[1] If you have an idea to improve this space, please email eppolito-at-math-dot-binghamton-dot-edu with your suggestion; I would like this space to be as useful to students as possible...
[2] APRIL FOOLS!