CS/Math 240: Introduction to Discrete Mathematics 8/6/2007

Exam 2 Handout

Instructor: Jeff Kinne TA: Mike Kowalczyk

The second exam will take place during the regular class time on the last day of class - Thursday, August 9. It will be closed book, closed notes, and no calculators allowed. You can prepare a 4x6 inch index card as a “cheat sheet” to use during the exam. You can write whatever you want onto it, or you can print off of a computer and paste onto the 4x6 card. The instructor will bring extra paper if you want scrap paper to write on.

Material on the Exam

The exam will cover material that was covered in lecture on probability and number theory - the lectures from July 11 through August 6. In addition to this material, there are a few things that you should remember from the first half of the course (although you won’t be tested specifically on anything from the first half).

Remember From First Half

Here is a list of items that I will assume you remember from the first half of the course.

- Proof Techniques. You should be able to use the “three standard proof techniques” - induction, contradiction, and direct proof.
- Set Theory. You should be able to apply rules for manipulating intersections, unions, and complements of sets (DeMorgan’s laws, distributive laws for intersection over union, inclusion-exclusion, etc.). These are often needed when computing probabilities of events.
- Algorithms. You should be able to use either induction or loop invariants to prove program correctness, and you should be able to analyze the running time of algorithms.

Examples of things you are *NOT* expected to remember for this exam: propositional logic, the algorithms covered in the first half of the course, graph theory, relations, recurrence relations. If you are unsure of whether a topic from the first half of the course is fair game on the second exam, please ask.

Probability Theory

You should be able to compute the probabilities of events occurring when a random experiment is performed. You should also be able to compute the expectation and variance of a random variable. In order to do both of these, the following are the main tools you should be able to use.

- Definition of Probability. You should know the definition of discrete probability ($\frac{|E|}{|S|}$) and be able to apply it.

- Rules for Counting. To apply the definition of probability, you should be able to use the various rules of counting: product rule, permutations, combinations, complement rule, disjoint events rule (sum rule), inclusion-exclusion.

- Probability Distributions. You should understand that probability can be defined by a probability distribution function, and should be able to apply this alternative definition. You should know basic facts and be able to reason about the binomial and geometric distributions.

- Conditional Probability. You should know the definition of conditional probability and independent events. You should also be able to apply the two main rules we developed for conditional probability: the Law of Total Probability, and Bayes' Theorem.

- Random Variables. You should understand how random variables are defined (perform a random experiment and assign a number to each outcome).

- Expectation and Variance. You should know the definitions of expectation and variance, and should be able to apply them. You should know the following rules for dealing with these: linearity of expectation, expectation of a product of independent random variables, variance of a sum of independent random variables, variance of a constant times a random variable.

- Estimating Probabilities. You should be able to use Markov's inequality and Chebyshev's inequality to estimate probabilities.

- Miscellaneous Rules. A few other rules of probability you should know: breaking up the probability of a conjunction of events by using definition of conditional probability, inclusion-exclusion rule for probability.

- Randomized Algorithm. You should be able to analyze the expected running time and success probability of simple randomized algorithms.

Integer Arithmetic

You should be able to reason about statements involving the integers, modular arithmetic, primes, etc. I will assume you recall the major theorems/lemmas we used during class and on homework assignments. If you do not remember some of these, I suggest you write them on your cheat sheet. Here are topics you should know.

1. Basic Algorithms. You should know that addition and multiplication can be done efficiently.

2. Size of Input. Be aware that if n is an integer, then it takes $O(\log n)$ bits to represent it. Then an algorithm running in $\Theta(\log n)$ time is polynomial in the size of the input, and an algorithm running in $\Theta(n)$ is exponential time.

3. Divisibility. You should know the definition of divisibility and be able to reason about simple facts involving divisibility.

4. Greatest Common Divisor. You should know the definition of gcd, the Euclidean algorithm, and the basic lemma used to prove the Euclidean algorithm is correct (if $a = b \cdot q + r$, then $gcd(a, b) = gcd(b, r)$). You should be able to reason about simple facts involving the gcd.

5. Modular Arithmetic. You should know the definition of mod, and being $\equiv$ mod m. You should know the definition of integer division, and know the statement of the "division algorithm" theorem. You should be able to perform basic modular arithmetic on small numbers (using the basic rules of modular arithmetic), and should be able to reason about simple facts involving modular arithmetic.

6. Primality. You should should be able to reason about simple statements involving primality. You should know the Prime Number Theorem and be able to apply it.

7. Chinese Remainder Theorem. You should know the statements of the two lemmas ($\exists s, t$ such that $gcd(a, b) = a \cdot s + b \cdot t$, and $\exists$ inverse of a mod m iff $gcd(a, m) = 1$) leading up to the Chinese remainder theorem and the theorem itself. You should be able to "execute" with small numbers the algorithm used to prove the theorem (the existence part of the proof). You should be able to reason about using the Chinese remainder theorem to perform large integer arithmetic.

8. Primality Testing. You should know Fermat's little theorem and be able to apply it.

Miscellaneous

There are certain miscellaneous facts that I will assume you know. If you don't know these, I suggest you write them on your cheat sheet.

- **Formulas for Arithmetic and Geometric Sums**
- **Telescoping Sums:** be able to look at a telescoping sum and cancel terms to get the final answer if all but a few terms cancel.
- **Rules of Exponents**
- **Rules of Logarithms**
- **Properties of the Integers:** + is associative, commutative, closed, has an identity (0), and is closed under inverse(-); * is associative, commutative, closed, has an identity(1), and is not closed under inverse(/); distributive law.

Study Helps

There are a number of sources that you can look to in studying for the exam.

- **Quizzes:** There are model solutions in the question feedback for each daily quiz.
- **Homeworks:** You have the model solutions from the homeworks. The exam questions won't necessarily be that difficult, but they're still a good reference.
- **Practice Exercises:** The practice exercises listed on the course website for each lecture would be excellent practice. They are all odd problems, so the answers are in the back of the book.

- **Sample Exam:** There is a sample exam on the course website that is also handed out in class. These problems will give you an idea of the difficulty of the questions. I suggest trying them out on your own, and then going to the exam review session to see how you did.

- **Exam Review Session:** Mike will hold an exam review session on Wednesday, August 8 from 12:30-2:00pm in 1325 CS. He will answer any questions you have, including going through the sample exam.

- **Suggested Readings:** The suggested readings for each day covers all the material we covered in class, in addition to some examples that we didn't cover in class. I point out that sometimes the suggested reading was modified after a lecture if we covered slightly different material in class than originally planned.