Final Review

Clay Thomas

May 7, 2015

This review set is by no means comprehensive. The best study study guide will be your notes and the homeworks.

1 Old Stuff

1. Draw a truth table for the following expressions:

   (a) $(p \wedge q) \rightarrow r$

   (b) $(p \wedge q) \vee (p \rightarrow q)$

   (c) $(p \wedge (p \rightarrow r) \wedge r) \vee (p \rightarrow r) \vee (r \vee \neg r)$

2. Prove that any binary function (a function accepting two inputs) from $\{0,1\} \times \{0,1\}$ to $\{0,1\}$ can be expressed in terms of $NAND$, which has the following truth table

p	q	$p\ NAND\ q$
0	0	1
0	1	1
1	0	1
1	1	0

3. Prove that given any 5 numbers, there exists some pair a, b of them such that $4|a-b$. (Hint[1])

4. Prove $\binom{n}{r} + \binom{n}{r+1} = \binom{n+1}{r+1}$.

5. Find a (good) asymptotic upper bound (big O) for the following functions:

   (a) $\frac{x^2+x-40}{x^{1.5}+1}$

   (b) $\Sigma_{k=1}^{n} \frac{1}{k}$

   (c) $\binom{2n}{n}$

[1] $4|a-b \iff a \equiv b \mod 4$. Then use the pigeonhole principle.

2 Counting

1. All of the following can be phrased in terms of "ways to put balls in jars". The jars and balls can both be distinguishable or indistinguishable. Figure out a general technique for each of the four possible combinations of distinguishable and indistinguishable. Note that there will not always be a simple formula: sometimes you have to just list certain possibilities. Some of the problems have less straight-forward followups.

   (a) How many ways can we put the textbooks for 5 different subjects in 3 garbage bins? We cannot tell the difference between the garbage bins for some reason.

   (b) George, Tom, Theodore, and Abe are playing a card game with a deck of 52 cards. At a given point in time, all 52 cards are in play but each player can have any number of cards (including zero). How many hand-configurations are there?

      i. How about if each player has 13 cards at a given point in time?

   (c) How many nonnegative integer solutions are there to the equation

   $$x + y + z + w = 20$$

   How many solutions are there for $x, y, z, w \geq 3$?

      i. We have three groups A,B,C full of identical objects. How many ways are there to pick n objects? The groups have an infinite number of objects (equivalently, we pick the objects with replacement).

   (d) How many ways are there to write 8 as the sum of 3 nonnegative integers written in nondecreasing order?

      i. How many ways are there to write 8 as the sum of (any number of) positive integers written in nondecreasing order?

2. Poker problems: Given a standard 52 card deck (13 faces (1 to 13) in each of 4 suits), how many five card hands result in the following poker hands:

   (a) Full house (3 of the same face and 2 of another face)

   (b) 3-of-a-kind (3 of the same face along with 2 different faces)

   (c) 4-of-a-kind (4 of the same face)

   (d) Flush (5 of the same suit)

   (e) Straight (5 consecutive faces (no "wrap around"))

   (f) Straight Flush (5 consecutive faces of the same suit)

   (g) Royal Flush (9 to 13 in the same face)

3 Probability

1. Prove that if E and F are independent, so are $\bar{E}$ and $\bar{F}$.

2. Prove that $P(A) = P(A|B)P(B) + P(A|\bar{B})P(\bar{B})$.

3. We are administering a test for some disease. We know that if a patient has the disease, there is a 99% probability that the test will be positive, however, if a patient does not have the disease there is a 4% chance the test will be positive. Furthermore, 0.1% of the population genuinely has the disease. What is the probability that a patient who tests positive actually has the disease? (Hint[2])

4. Find and prove the formulas for geometric and binomial distributions. If you are feeling ambitions, find the expected values and variances, although this will likely involve calculus.

5. Prove that if $P(A) = 0.8$ and $P(F) = 0.6$,

   (a) $P(E \cap F) \geq 0.4$

   (b) $P(E \cup F) \geq 0.8$. (There is a more general result behind this one. What is it?)

6. A family has 2 children and one is a girl. What is the probability that they are both girls?

4 Number Theory

1. Prove that $n-1$ is its own multiplicative inverse modulo n (more specifically, $(n-1)(n-1) \equiv 1 \mod n$).

2. Find the following modular inverses, or state that they do not exist (given an a, $a^{-1} \mod n$ is the number such that $aa^{-1} \equiv 1 \mod n$)

   (a) $3^{-1} \mod 6$

   (b) $3^{-1} \mod 5$

   (c) $24^{-1} \mod 35$

   (d) $35^{-1} \mod 24$

3. Solve the following modular congruences

   (a) $135x \equiv 3 \mod 56$

   (b) $24x \equiv 7 \mod 35$

4. Solve the following systems of linear congruences.

[2] Bayes' theorem plus problem 2

(a) The following system of four equations:

$$x \equiv 4 \mod 5$$

$$x \equiv 4 \mod 7$$

$$x \equiv 4 \mod 11$$

$$x \equiv 4 \mod 13$$

(b) Here's a system of 3 equations

$$x \equiv 2 \mod 7$$

$$x \equiv 8 \mod 9$$

$$x \equiv 16 \mod 32$$

(c) And finally, here's two. Note that you should only use the extended Euclidean algorithm once to finish this problem

$$x \equiv 12 \mod 35$$

$$x \equiv 18 \mod 32$$

5. Compute
$$12^{43} \mod 9$$

6. Compute
$$12^{1342} \mod 7$$

   Hint: this one is easier than the last one.[3]

7. Compute
$$3^{1235871238576182836872} \mod 11$$

   Hint: This one is even easier.

8. Choose two (manageable small) prime numbers p and q and compute everything necessary for RSA encryption. Send a number m as a message. Check that the message decrypts properly.

[3] Fermat.

5 State Machines

The main point of thinking about finite state machines is that we come to some realizations about what it means to compute things and what tools we need. Because there are only a finite number of possible states (and thus a finite amount of "memory"), we cannot compute everything we might want to.

Draw deterministic finite state machine to recognize the following sets of strings:

1. The language consisting of only the empty string.
2. The set of strings in the alphabet $\{a, b, c\}$ that have a as their third letter and end in the sequence abc.
3. The set of valid binary numbers (possibly with decimal points).
4. The set of strings over $\{a, b, c\}$ that DO NOT contain abc as a substring.

Draw nondeterministic finite automata to recognize the following:

1. The set of strings of characters in $\{a, b, c\}$ that end in palindromes of length three.
2. The set of strings of as and bs that either end with a or start with b.
3. The set of strings of as and bs that either end with aa or have b as their second letter.

Now find some already-written finite automata and determine what languages they accept.