Computer Science Foundation Exam

December 14, 2012

Section II B

DISCRETE STRUCTURES

NO books, notes, or calculators may be used,
and you must work entirely on your own.

SOLUTION

Question	Max Pts	Category	Passing	Score
1	15	CTP (Counting and Probability)	10	
2	15	PRF (Relations)	10	
3	15	PRF (Functions)	10	
4	15	NTH (Number Theory)	10	
ALL	60	---	40	

You must do all 4 problems in this section of the exam.

Problems will be graded based on the completeness of the solution steps and <u>not</u> graded based on the answer alone. Credit cannot be given unless all work is shown and is readable. Be complete, yet concise, and above all <u>be neat</u>.

1) (15 pts) CTG (Counting and Probability)

(a) (5 pts) How many different strings can be made from the word "PEPPERCORN"?

(b) (10 pts) A pair of dice are rolled in a remote location and when you ask an honest observer whether at least one die came up "6", this honest observer answers "yes". What is the probability that the sum of the numbers that came up on the two dice is 8, given the information provided by the honest observer?

Note: Please leave your answers in factorials, permutations, combinations and powers. Do not calculate out the actual numerical value for any of the questions.

<u>Solution (a)</u>
This is a permutation with repetition question. There is 1 C, 2 Es, 1 N, 1 O, 3 Ps, and 2 Rs, Plugging into the proper formula we have $\frac{10!}{2!3!2!} = 151200$. (Grading: 2 pts for recognizing which formula to use, 3 pts for properly plugging into it, solution should be left in factorials, but either answer can be accepted.)

<u>Solution (b)</u>
This is a conditional probability question. Given that a 6 appears on one of the dice, there are 11 possible rolls that could have occurred: (1, 6), (2, 6), (3, 6), (4, 6), (5, 6), (6, 6), (6, 5), (6, 4), (6, 3), (6, 2), and (6, 1). Of this sample space, two of them (2, 6) and (6, 2) are rolls that add up to 8. It follows that the desired probability is $\frac{2}{11}$.

<u>Alternate Solution (b)</u>
Using the definition of conditional probability, we find that the desired probability is $\frac{p(one\ die=6\ and\ sum=8)}{p(one\ die=6)}$. The probability of the bottom occurring is $1 - (\frac{5}{6})^2 = \frac{11}{36}$, because the probability of NOT rolling any sixes is the probability of not rolling a 6 twice in a row. (This probability is $(\frac{5}{6})^2$ since the two die rolls are independent.) To get our desired probability we subtract the previous answer from 1. The probability of one die equaling 6 and the sum being 8 is $\frac{2}{36}$, since there are 36 possible pairs of dice of which 2 of them (2, 6) and (6, 2), have a die with the value 6 and sum to 8. We obtain the final answer as follows: $\frac{2/36}{11/36} = \frac{2}{11}$.

Grading: 2 points for the recognition of a conditional probability, 4 points for the denominator, 4 points for the numerator.

2) (15 pts) PRF (Relations)

(a) (12 pts) A relation $\boldsymbol{R}$ on set $\boldsymbol{A}$ is called *circular* if, for any $a, b, c \in \boldsymbol{A}$**,** a $\boldsymbol{R}$ b and b $\boldsymbol{R}$ c then c $\boldsymbol{R}$ a. Please prove that if $\boldsymbol{R}$ is reflexive and circular then $\boldsymbol{R}$ is an equivalence relation.

(b) (3 pts) Let $\boldsymbol{R}$ be the relation defined on the set of integers where a $\boldsymbol{R}$ b means that $a \equiv c \ (mod\ 5)$. Find $[4]_{\boldsymbol{R}}$.

<u>Solution (a)</u>

We must prove that R is reflexive, symmetric and transitive.

<u>Reflexive:</u> This is given to us in the problem statement, so it's true. **(1 pt)**

<u>Symmetric:</u> We must show that if a $\boldsymbol{R}$ b, then b $\boldsymbol{R}$ a. **(1 pt)**

For arbitrary elements a and b in A, assume a $\boldsymbol{R}$ b. **(1 pt)**

Since R is reflexive, it follows that b $\boldsymbol{R}$ b. **(1 pt)**

Since R is circular, if we plug in c = b into the definition, we see that since a $\boldsymbol{R}$ b and b $\boldsymbol{R}$ b, it follows that b $\boldsymbol{R}$ a. This proves that R is symmetric. **(2 pts)**

<u>Transitive:</u> We must show that if a $\boldsymbol{R}$ b and b $\boldsymbol{R}$ c then a $\boldsymbol{R}$ c. **(1 pt)**

For arbitrary elements a, b and c in A, assume a $\boldsymbol{R}$ b and b $\boldsymbol{R}$ c. **(1 pt)**

Since R is circular, it follows that c $\boldsymbol{R}$ a. **(2 pts)**

But, we ALSO know that R is symmetric. Thus, if c $\boldsymbol{R}$ a, via symmetry, we have a $\boldsymbol{R}$ c, as desired. Thus, R is transitive. **(2 pts)**

This proves that R is an equivalence relation.

<u>Solution (b)</u>

$[4]_{\boldsymbol{R}}$ = […,-6, -1, 4, 9, …] or
$[4]_{\boldsymbol{R}}$ = { 4 + 5n | n ∈ Z }

The first is acceptable because it shows that the set is infinite and reasonably explains the pattern to generate all values. The second is preferred since it's unambiguous. (Grading: Generally all or nothing, but give partial credit if you see fit.)

3) (15 pts) PRF (Functions)

(a) (8 pts, 2 pts each) Determine whether $f : \mathbf{Z} \rightarrow \mathbf{Z}$ is injective (one-to-one), surjective (onto), bijective (both), or none

i. $f(n) = n - 1$
ii. $f(n) = n^2 + 1$
iii. $f(n) = n^3$
iv. $f(n) = \left\lceil \frac{n}{2} \right\rceil$

(b) (7 pts) Given three sets *A*, *B*, and *C*. Suppose that *f* is a function from *A* to *B* and *g* is a function from *B* to *C*. Prove that if $g \circ f$ is an onto (surjective) function, then *g* is an onto (surjective) function.

Solution (a)
(i) bijective – graph is a line
(ii) neither – since the domain is integers, many y values are never achieved. Also, f(-1)=f(1).
(iii) injective – since the domain is integers, many y values are never achieved.
(iv) surjective – for any integer y, f(2y) = y.

Grading: 2 pts for each part, all or nothing, no reasons are necessary

Solution (b)
Let's use proof by contradiction. Assume to the contrary that g isn't surjective. **(1 pt)**

This means that there exists a value c ∈ C such that there is no value x for which g(x) = c. **(2 pts)**

Since we are given that $g°f$ is surjective, it follows that there exists some value a ∈ A such that g(f(a)) = c. But this implies that for a specific value b = f(a), g(b) = c, contradicting our assumption that there doesn't exist some value x for which g(x) = c. **(3 pts)**

It follows that our original assumption is incorrect and g is surjective. **(1 pt)**

Alternate Solution (b)
Use direct proof. **(1 pt)**

Given that $g°f$ is surjective, it follows that for any value c ∈ C, there exists some value a ∈ A such that g(f(a)) = c. **(3 pts)**

Let b = f(a). It follows that g(b) = c, proving that g is surjective. **(2 pts)**

Namely, for an arbitrarily chosen value of c in C, we can always find a value b in B such that g(b) = c. **(1 pt)**

4) (15 pts) NTH (Number Theory)

(a) (9 pts) Given a prime number p and we know that $n^2 \equiv n \ (\mathbf{mod}\ p)$.

(i) (6 pts) Prove that $n \equiv 0 \ (\mathbf{mod}\ p)$ or $n \equiv 1 (\mathbf{mod}\ p)$

(ii) (3 pts) Show the previous statement is not necessary true if p is not prime by a counter example.

(b) (6 pts) Use Euclidean Algorithm to find the greatest common divisor (GCD) of 290 and 68.

Solution (a)

(i) Taking our original equation, we have:

$n^2 \equiv n \ (\mathbf{mod}\ p)$
$n^2 - n \equiv 0 \ (\mathbf{mod}\ p)$ **(1 pt)**
$n(n-1) \equiv 0 \ (\mathbf{mod}\ p)$ **(1 pt)**

This is equivalent to p | (n(n – 1)). **(1 pt)**

Since p is prime and can't be divided itself, it follows that either p | n or p | (n – 1). **(1 pt)**

In the first case, n ≡ 0 $(\mathbf{mod}\ p)$. **(1 pt)**
In the second case n – 1 ≡ 0 $(\mathbf{mod}\ p)$, so n ≡ 1 $(\mathbf{mod}\ p)$, as desired. **(1 pt)**

(ii) Let p = 6 and n = 3. We have $n^2 - n = 3^2 - 3 = 6 \equiv 0 \ (\mathbf{mod}\ 6)$, but n ≡ 3 $(\mathbf{mod}\ 6)$.

Solution (b)

290 = 4 x 68 + 18 **(1 pt)**
68 = 3 x 18 + 14 **(1 pt)**
18 = 1 x 14 + 4 **(1 pt)**
14 = 3 x 4 + 2 **(1 pt)**
4 = 2 x 2 **(1 pt)**
GCD(290, 68) = 2. **(1 pt)**