Computer Science Foundation Exam

May 2, 2014

Section II A

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	PRF (Induction)	10	
2	10	PRF (Logic)	6	
3	15	PRF (Sets)	10	
4	10	NTH (Number Theory)	6	
ALL	50		32	

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 not 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 be neat.

1) (15 pts) PRF (Induction)

Use mathematical induction on n to show that $64 \mid (9^n - 8n - 1)$ for all non-negative integers n.

Let $f(n) = 9^n - 8n - 1$.

Base case: $n = 0$. $f(n) = 9^0 - 8(0) - 1 = 1 - 0 - 1 = 0$. Since $64 \times 0 = 0$, $64 \mid f(0)$, proving the base case. (Grading: 2 pts)

Inductive hypothesis: Assume for an arbitrary non-negative integer $n = k$ that $64 \mid (9^k - 8k - 1)$. (Grading: 2 pts)

Inductive step: Prove for $n = k + 1$ that $64 \mid (9^{k+1} - 8(k+1) - 1)$. (Grading: 2 pts)

$$\begin{aligned}
9^{k+1} - 8(k+1) - 1 &= 9(9^k) - 8k - 8 - 1 && \text{(1 pt)}\\
&= 9(9^k) - 8k - 64k + 64k - 9 && \text{(3 pts)}\\
&= 9(9^k) - 72k - 9 + 64k &&\\
&= 9[(9^k) - 8k - 1] + 64k && \text{(2 pts)}\\
&= 9(64c) + 64k, \text{ for some integer c using the inductive hypothesis} && \text{(2 pts)}\\
&= 64(9c + k) && \text{(1 pt)}
\end{aligned}$$

Since c and k are integers, we've shown that $64 \mid (9^{k+1} - 8(k+1) - 1)$, as desired.

2) (10 pts) PRF (Logic)

Let P(x), Q(x) and R(x) be open statements for the universe of integers that satisfy the following premise: $\forall x[P(x) \rightarrow (Q(x) \vee R(x))]$.

Can we conclude $(\forall x[P(x) \rightarrow Q(x)]) \vee (\forall x[P(x) \rightarrow R(x)])$?

If so, prove it, if not, provide a specific counter-example with statements representing P(x), Q(x) and R(x), explaining why the chosen set of statements doesn't satisfy the conclusion shown.

This is false. Consider the following open statements P(x), Q(x) and R(x) for the universe of integers:

P(x): x is an integer
Q(x): x is an even integer
R(x): x is an odd integer

Clearly, for all integers x, either Q(x) is true or R(x) is true, thus, it follows that for this specific example, $\forall x[P(x) \rightarrow (Q(x) \vee R(x))]$ is true.

However, consider these component statements: (a) $(\forall x[P(x) \rightarrow Q(x)]$ and (b) $(\forall x[P(x) \rightarrow R(x)]$. Neither of them is true. For all x, it is not the case that x is even. Also, for all x, it is not the case that x is odd. Plugging in x = 1 disproves (a) and plugging in x = 2 disproves (b).

The key here is that neither Q(x) nor R(x) follows all the time, but one of the two conditions does hold for all x. The converse statement is true however, if $(\forall x[P(x) \rightarrow Q(x)]) \vee (\forall x[P(x) \rightarrow R(x)])$, it will always be the case that $\forall x[P(x) \rightarrow (Q(x) \vee R(x))]$.

Grading: 2 pts max for trying to prove the assertion, points for disproof are as follows: 2 pts for saying it's false. 3 pts for clearly specifying a set of open statements for P, Q and R, 2 pts for these statements being a valid counter example, and 3 pts for the proof that they are indeed a counter-example.

3) (15 pts) PRF (Sets)

Prove or disprove the following assertion about finite sets A and B:

$$P(A) \cap P(B) = P(A \cap B)$$

Recall that *P(A)* is simply the set of all subsets of A.

This statement is true. (Grading: 1 pt) We will prove it in two steps, by showing:

(a) $P(A) \cap P(B) \subseteq P(A \cap B)$ (2 pts)
(b) $P(A \cap B) \subseteq P(A) \cap P(B)$ (2 pts)

We use direct proof for both sides.

To prove (a), consider an arbitrary element $X \in P(A) \cap P(B)$. (1 pt) By definition, $X \in P(A) \wedge X \in P(B)$. (1 pt) By definition of power set, we have $X \subseteq A \wedge X \subseteq B$. (1 pt) By definition of set intersection, we have $X \subseteq (A \cap B)$. (1 pt) Finally, by definition of power sets, we find that $X \in P(A \cap B)$, as desired. (1 pt)

To prove (b), consider an arbitrary element $X \in P(A \cap B)$. (1 pt) By definition of power set, we have that $X \subseteq (A \cap B)$. (1 pt) By definition of set intersection, we have $X \subseteq A \wedge X \subseteq B$. (1 pt) Finally, by definition of power set, we have $X \in P(A) \wedge X \in P(B)$. (1 pt) Last, by definition of union, we have $X \in P(A) \cap P(B)$, as desired. (1 pt)

Note: Many other methods may be used to prove this statement. Please grade accordingly. Also, both sides don't need to be presented if it's proven that each step is "reversible." This is a bit tricky though!

4) (10 pts) NTH (Number Theory)

Let a and n be relatively prime positive integers. (Thus, gcd(a, n) = 1.) Consider the set S = $\{ai | i \in Z, 0 \leq i < n\}$. Prove that each value in S is unique mod n. You may use the following theorem in your proof: If x | (yz), and gcd(x, y) = 1, then x | z. (Hint: Use proof by contradiction and assume that two distinct values in the set are equivalent mod n. If two values are equivalent mod n, then their difference is divisible by n.)

Assume to the contrary that two unique values in S are equivalent mod n. Let these values be ai and aj, where $0 \leq i \neq j < n$. (Grading: 2 pts) Since they are equivalent mod n, we have:

ai ≡ aj (mod n) (Grading: 1 pt)
ai – aj ≡ 0 (mod n) (Grading: 1 pt)
a(i – j) ≡ 0 (mod n) (Grading: 1 pt)

By definition of mod, we have n | (a(i– j)). Since gcd(a, n) = 1, using the given theorem, we conclude that n | (i – j). (Grading: 2 pts)

Remember that $0 \leq i, j < n$. Thus, $|i – j| < n$. But, n | (i – j) and $|i – j| < n$ infers that 0 = i – j, since it's the only integer divisible by n in the interval [-n+1, n – 1]. (Grading: 2 pts) This contradicts our assumption that $i \neq j$. (Grading: 1 pt)

This means that there must be a flaw in our proof. The only step that wasn't necessarily justified was the very first assumption, that two values in the set are equivalent mod n. Thus, this assumption is incorrect and we've proven that no two values in the set S are equivalent mod n.