Computer Science Foundation Exam

August 14, 2015

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 <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) PRF (Induction)

Use mathematical induction to prove that, for every positive integer n,

$$3 \mid (5^n + (-1)^{n+1})$$

Let P(n) be an open statement equal to the proposition above.

Base Case (n=1):
$5^1 + (-1)^2 = 5 + 1 = 6 = 3(2)$
$3 \mid 3(2)$ by definition of divisible. **(Grading: 2 pts)**

Inductive Hypothesis:
Assume $P(k)$ is true for all $k, 2 \leq k$ In other words, assume the following: **(Grading: 2 pts)**

$$3 \mid (5^k + (-1)^{k+1})$$

Inductive step (show true for n=k+1): **(Grading: 2 pts)**
Let $a = 5^{k+1} + (-1)^{k+1+1} = 5^{k+1} + (-1)^{k+2}$

Our goal is to show that $3 \mid a$. **(Grading: 6 pts - 2 pts per step, roughly)**

$$a = 5^{k+1} + (-1)^{k+2} = 5 \cdot 5^k + (-1)(-1)^{k+1} = (6-1)(5^k) + (-1)(-1)^{k+1}$$
$$= 6(5^k) + (-1)(5^k + (-1)^{k+1})$$

To simplify things, we can use two variables b and c:

$$b = 6(5^k), c = (-1)(5^k + (-1)^{k+1})$$

By manipulating b, it follows $b = 6(5^k) = 3 \cdot 2 \cdot (5^k)$, By definition of divisible, we know $3 \mid b$. **(Grading: 1 pt)**

By the inductive hypothesis and the multiplicative divisibility law, it follows that $3 \mid c$. **(Grading: 2 pts use of IH)**

By the additive divisibility law it follows that $3 \mid (b + c)$. **(No need to state the law…)**

$$\therefore 3 \mid a$$

By the principle of mathematical induction, our conjecture holds.

$$Q.E.D.$$

2) (15 pts) PRF (Logic)

Validate the following argument using the laws of logic, substitution rules or rules of inference. List the rule used in each step and label the steps used in each derivation.

$$\begin{array}{l} (p \vee r) \rightarrow q \\ \neg s \\ (p \wedge r) \vee s \\ \neg q \vee t \\ \hline \therefore t \end{array}$$

1.	$\neg s$	Premise
2.	$(p \wedge r) \vee s$	Premise
3.	$p \wedge r$	Disjunctive Syllogism on (1) and (2)
4.	$(p \vee r) \rightarrow q$	Premise
5.	p	Simplification on (3)
6.	$p \vee r$	Disjunctive Amplification on (5)
7.	q	Modus Ponens on (4) and (6)
8.	$\neg q \vee t$	Premise
9.	t	Disjunctive Syllogism on (7) and (8)

$Q.E.D.$

Grading: -1 per incorrect step, -1/2 per incorrect reason, give 0 if left blank.

3) (10 pts) PRF (Sets)

Prove the following statement is true:

Let A and B be two finite sets. Prove that $A \nsubseteq B \Rightarrow A \neq \emptyset \wedge \Big(\exists x \left(x \in (A \cup B)\right)\Big)$.

Proving the contrapositive is equivalent to proving the original statement:

$$\neg\Big(A \neq \emptyset \wedge \Big(\exists x \left(x \in (A \cup B)\right)\Big)\Big) \rightarrow A \subseteq B$$

Next rework the premise using DeMorgan's law for quantifiers and Logical DeMorgan's law:

$$A = \emptyset \vee \Big(\forall x \left(x \notin (A \cup B)\right)\Big) \rightarrow A \subseteq B$$

Use DeMorgan's law to simplify the above statement:

$$A = \emptyset \vee \big(\forall x \left(x \notin A \wedge x \notin B\right)\big) \rightarrow A \subseteq B$$

The Universal quantified statement is the same as the definition of empty set. So we can rework this statement further:

$$A = \emptyset \vee (A = \emptyset \wedge B = \emptyset) \rightarrow A \subseteq B$$

As everything here is a proposition, we can use the Absorption Law from the Laws of Logic to obtain the following:

$$A = \emptyset \rightarrow A \subseteq B$$

As we only used logical equivalences to rework our statement, proving this statement is equivalent to the original.

Our goal is to prove $A \subseteq B$. To show this we need to show the following is true:

$$\forall x \left(x \in A \rightarrow x \in B\right)$$

This statement holds vacuously as there are no elements in A. This is determined from the premise $A = \emptyset$.

$$Q.E.D.$$

Alternate solution:

Use direct proof. If A isn't a subset of B, there must exist some element of x such that $x \in A$ and $x \notin B$. Thus, it follows that A is non-empty (since it contains x). By definition of union it also follows that $x \in (A \cup B)$, completing the proof.

Grading: Many, many ways to do this, conceptually, grade as follows:
5 pts for showing that that A is non-empty,
5 pts for showing that A union B is non-empty.

4) (10 pts) NTH (Number Theory)

Prove for an arbitrary prime number p that there always exists some composite number q where $\gcd(p, p+q) > 1$.

First we will convert the English statement into a Quantified Statement:

$$\forall p \left(p \; is \; prime \rightarrow \; \exists q \; (q \; is \; composite \; \wedge \gcd(p, p+q) > 1)\right)$$

So for an arbitrary p, we must find a specific q that is composite and the gcd statement above holds. Let q be set by the below equation:

$$q = 2p$$

This value of q is not prime as it contains the divisor 2 in addition to 1 and $2p$. A composite number is a positive integer > 1 that is not prime. The established q meets that criteria.

Now we merely need to show that q will satisfy our gcd inequality:

$$\gcd(p, p+q) = \gcd(p, p+2p) = \gcd(p, 3p)$$

As p is prime, the gcd of the above statement must be either 1 or p as these are the only options for the divisor. We know $p \mid 3p$ by definition of divisible. As $p > 1$, due to p being prime, it follows:

$$\gcd(p, 3p) = \text{p}$$

As we have shown there always exists a satisfactory q for all p, our proof is complete.

$$Q.E.D.$$

Grading: 5 pts for picking a value of q. 5 pts for showing that the corresponding gcd is greater than 1.