Math for CS 2015/2019 Midterm 2 solutions

https://github.com/spamegg1

June 13, 2022

Contents

1 Problem 1 (Structural Induction)

Definition 1. *The set RAF of rational functions of one real variable is the set of functions defined recursively as follows:*

Base cases:

The identity function, $id(r) ::= r$ *for* $r \in \mathbb{R}$ *(the real numbers), is an RAF,*

any constant function on $\mathbb{R}$ *is an RAF.*

Constructor cases: *If f, g are RAF's, then so are $f \,\boldsymbol{op}\, g$, where $\boldsymbol{op} = +, /, \cdot$.*

Prove by structural induction that RAF is closed under composition. That is, using the induction hypothesis,

$$P(h) ::= \forall g \in \text{RAF},\ h \circ g \in \text{RAF}$$

prove that $P(h)$ holds for all $h \in$ RAF. Make sure to indicate explicitly

each of the base cases, and

each of the constructor cases.

Hint: A proof in terms of op covers all the cases.

Proof. **Base Cases.**

First we want to prove $P(h)$ where h is the identity function id.

1. Assume $g \in$ RAF.
2. Consider the function $id \circ g$. This is defined as

$$(id \circ g)(x) ::= id(g(x)) = g(x) \text{ for all } x \in \mathbb{R}$$

3. So $id \circ g$ is actually the same function as g. Therefore $id \circ g \in$ RAF.
4. Since g was arbitrary, (3) holds for all $g \in$ RAF, so $P(id)$ is true.

Second we want to prove $P(h)$ where h is any constant function on $\mathbb{R}$.

1. Assume h is any constant function, in other words assume $c \in \mathbb{R}$ and $h(x) = c$ for all $x \in \mathbb{R}$. By the Base Cases of the definition, $h \in$ RAF.
2. Assume $g \in$ RAF.
3. Consider the function $h \circ g$. This is defined as

$$(h \circ g)(x) ::= h(g(x)) = c \text{ for all } x \in \mathbb{R}$$

4. So $h \circ g$ is actually the same function as h. Therefore $h \circ g \in$ RAF.
5. Since g was arbitrary, (4) holds for all $g \in$ RAF, so $P(h)$ is true.

Induction Step.

1. Assume $h_1, h_2 \in$ RAF, and assume $P(h_1)$ and $P(h_2)$ are true. We want to prove that $P(h_1\ op\ h_2)$ is true, where $op = +, /, \cdot$.
2. Assume $g \in$ RAF.
3. Consider the function $(h_1\ op\ h_2) \circ g$. This is defined as

$$((h_1\ op\ h_2) \circ g)(x) = (h_1\ op\ h_2)(g(x)) = h_1(g(x))\ op\ h_2(g(x)) \text{ for all } x \in \mathbb{R}$$

4. Since $P(h_1)$ is true, the function $(h_1 \circ g)(x) = h_1(g(x))$ is in RAF.

5. Since $P(h_2)$ is true, the function $(h_2 \circ g)(x) = h_2(g(x))$ is in RAF.

6. By (4) and (5) and the Constructor Cases of the definition, the function $f(x) = h_1(g(x))\ op\ h_2(g(x))$ is also in RAF.

7. Since g was arbitrary, (6) holds for all $g \in$ RAF, therefore $P(h_1\ op\ h_2)$ is true.

Conclusion

By the Base Cases and the Induction Step, and the principle of Structural Induction, $P(h)$ holds for all $h \in$ RAF. □

2 Problem 2 (State Machines)

The Stata Center's delicate balance depends on two buckets of water hidden in a secret room. The big bucket has a volume of 25 gallons, and the little bucket has a volume of 10 gallons. If at any time a bucket contains exactly 13 gallons, the Stata Center will collapse. There is an interactive display where tourists can remotely fill and empty the buckets according to certain rules. We represent the buckets as a state machine.

The state of the machine is a pair (b, l), where b is the volume of water in big bucket, and l is the volume of water in little bucket.

2.1 (a)

(a) We informally describe some of the legal operations tourists can perform below. Represent each of the following operations as a transition of the state machine. The first is done for you as an example.

1. Fill the big bucket.

$$(b, l) \to (25, l)$$

2. Empty the little bucket.

3. Pour the big bucket into the little bucket. You should have two cases defined in terms of the state (b, l) if all the water from the big bucket fits in the little bucket, then pour all the water. If it doesn't, pour until the little jar is full, leaving some water remaining in the big jar.

Proof. (1) is done, so we do (2) and (3).

2. Empty the little bucket:

$$(b, l) \to (b, 0)$$

3. Pour the big bucket into the little bucket.

$$(b, l) \to (0, b + l) \text{ if } b \leq 10 - l$$

$$(b, l) \to (b - (10 - l), 10) \text{ if } b > 10 - l$$

□

2.2 (b)

(b) Use the Invariant Principle to show that, starting with empty buckets, the Stata Center will never collapse. That is, the state $(13, x)$ in unreachable. (In verifying your claim that the invariant is preserved, you may restrict to the representative transitions of part (a).)

Proof. We want to prove that the following condition is always true for all states (b, l):

$$P(b, l) ::= b \neq 13$$

If you think about it, starting with empty buckets of capacities 25 and 10, where we are only allowed to fill/empty buckets completely, or pour big bucket into the small bucket, the amounts in the buckets should always remain divisible by 5.

So let's prove this stronger condition which will help us in the proof:

$$P(b, l) ::= 5 \mid b \text{ AND } 5 \mid l$$

1. First we prove it for the initial state of empty buckets $(b, l) = (0, 0)$: indeed, $5 \mid 0$ and $5 \mid 0$, so $P(0, 0)$ holds.

2. Now we prove that the condition is preserved through transitions. For the rest of the proof, assume $P(b, l)$ holds, so $5 \mid b$ and $5 \mid l$.

3. We want to show $P(25, l)$ holds. Notice that $5 \mid 25$ and $5 \mid l$, so $P(25, l)$ also holds. This shows that the condition is preserved through transition 1.

4. We want to show $P(b, 0)$ holds. Since $5 \mid b$ and $5 \mid 0$, $P(b, 0)$ also holds. So the condition is preserved through transition 2.

5. Now assume $b \leq 10 - l$. We want to show $P(0, b + l)$ holds. First we notice $5 \mid 0$. Second, since $5 \mid b$ and $5 \mid l$, we also have $5 \mid (b + l)$. So $P(0, b + l)$ holds. So the condition is preserved through the first case of transition 3.

6. Now assume $b > 10 - l$. We want to show $P(b - (10 - l), 10)$ holds. First notice $5 \mid 10$. Also, $b - (10 - l) = b - 10 + l$. Since $5 \mid b$, $5 \mid l$ and $5 \mid -10$, we have $5 \mid (b - 10 + l)$. Therefore $P(b - (10 - l), 10)$ holds. So the condition is preserved through the second case of transition 3.

7. By the above steps and Floyd's Invariant Principle, $P(b, l)$ holds for all states (b, l).

8. Therefore the amounts in the buckets are always divisible by 5, which means the amount of water in a bucket can never equal 13. □

3 Problem 3 (Jections)

Prove that if A is an infinite set and B is a countably infinite set that has no elements in common with A, then

$$A \text{ bij } (A \cup B)$$

Reminder: You may assume any of the results from class, MITx, or the text as long as you state them explicitly.

Proof. Since B is countable, fix an enumeration $b_0, b_1, \ldots$ of elements of B.

1. Case 1: A is countable. Fix an enumeration $a_0, a_1, \ldots$ of elements of A.

2. Then a bijection $f : A \to (A \cup B)$ is given as follows: for all $i \in \mathbb{N}$ define

$$f(a_{2i+1}) = a_i \text{ and } f(a_{2i}) = b_i$$

So the odd indexed a_is get mapped to A and even indexed a_is get mapped to B. It is easy to see that this is a bijection.

3. Case 2: A is uncountable.

We can actually use the same idea in this case. Basically, the idea is that A contains at least a countably infinite subset. We can do the even/odd trick to map this subset to itself plus B.

4. By Theorem 7.1.5 either A surj $\mathbb{N}$ or $\mathbb{N}$ surj A. Since A is uncountable, $\mathbb{N}$ surj A is not possible (otherwise A is countable).

5. So A surj $\mathbb{N}$, which implies there is an injection $f : \mathbb{N} \to A$. Consider the range of f, let's call it A', which is a countable subset of A. Fix an enumeration $a_0, a_1, \ldots$ of A'.

6. Define a function $g : A \to (A \cup B)$ as follows:

$$\begin{array}{rcl} g(a_{2i+1}) & = & a_i \quad \text{for } i \in \mathbb{N} \\ g(a_{2i}) & = & b_i \quad \text{for } i \in \mathbb{N} \\ g(a) & = & a \quad \text{if } a \notin A' \end{array}$$

It is easy to see that g is a bijection.

Note that the two cases are actually not necessary; the proof in Case 2 works for all A (the injection f exists for all infinite A, not just uncountable A). But I included it to ease you into the idea. □

4 Problem 4 (GCDs)

Let

$$m = 2^9 \cdot 5^{24} \cdot 7^4 \cdot 11^7$$
$$n = 2^3 \cdot 7^{22} \cdot 11^{211} \cdot 19^7$$
$$p = 2^5 \cdot 3^4 \cdot 7^{6042} \cdot 19^{30}$$

4.1 (a)

What is the $\gcd(m, n, p)$?

Proof. The only primes common in all 3 numbers are 2 and 7. The GCD should be the product of the smallest powers of those primes occurring in the 3 numbers. So the GCD is:

$$2^3 \cdot 7^4$$

□

4.2 (b)

What is the least common multiple, $\text{lcm}(m, n, p)$?

Proof. All of the primes that occur in any one of the 3 numbers are 2, 3, 5, 7, 11, 19. The LCM should be the product of the biggest powers of those primes occurring in any one of the 3 numbers. So the LCM is:

$$2^9 \cdot 3^4 \cdot 5^{24} \cdot 7^{6042} \cdot 11^{211} \cdot 19^{30}$$

□

Let $v_k(n)$ be the largest power of k that divides n, where $k > 1$. That is,

$$v_k(n) ::= max\{i \mid k^i \text{ divides } n\}$$

If A is a nonempty set of nonnegative integers, define

$$v_k(A) ::= \{v_k(a) \mid a \in A\}$$

4.3 (c)

Express $v_k(gcd(A))$ in terms of $v_k(A)$.

Proof. First let's work with some examples.

$$v_2(2^9 \cdot 3^4 \cdot 5^{24} \cdot 7^{6042} \cdot 11^{211} \cdot 19^{30}) = 9$$

$$v_7(2^9 \cdot 3^4 \cdot 5^{24} \cdot 7^{6042} \cdot 11^{211} \cdot 19^{30}) = 6042$$

etc. Now let's apply it to some sets. Define $A = \{m, n, p\}$. Then

$$v_2(A) = \{9, 3, 5\}$$

$$v_7(A) = \{4, 22, 6042\}$$

etc. To get the GCD of a set of numbers, for each prime that is common to all of the numbers in the set, we would choose the smallest power of that prime that occurs in one of the numbers.

For example, $v_2(A) = \{9, 3, 5\}$ and the power of 2 that appears in the GCD of A is 3, because that's the smallest. So:

$$v_k(gcd(A)) = \min v_k(A)$$

This reasoning also works when k is not prime. □

4.4 (d)

Let p be a prime number. Express $v_p(lcm(A))$ in terms of $v_p(A)$.

Proof. By a similar argument,

$$v_p(lcm(A)) = \max v_p(A)$$

□

4.5 (e)

Give an example of integers a, b where $v_6(lcm(a, b)) > \max(v_6(a), v_6(b))$.

Proof. Let $a = 2^2 \cdot 3$ and $b = 2 \cdot 3^2$. So $v_6(a) = v_6(b) = 1$. Then $lcm(a, b) = 36$ and $v_6(lcm(a, b)) = 2$ which is greater than $\max(v_6(a), v_6(b)) = 1$. □

5 Problem 5 (Congruences)

Prove that if $a \equiv b \ (mod\ 14)$ and $a \equiv b \ (mod\ 5)$, then $a \equiv b \ (mod\ 70)$.

Proof. 1. Assume $a \equiv b \ (mod\ 14)$ and $a \equiv b \ (mod\ 5)$.

2. Since $a \equiv b \ (mod\ 14)$, by definition of mod, there exists an integer k such that $a = 14k + b$.

3. Since $a \equiv b \ (mod\ 5)$, by definition of mod, there exists an integer m such that $a = 5m + b$.

4. By (2) and (3), $a - b = 14k = 5m$. Since 5 does not divide 14, 5 divides k.

5. So there exists an integer n such that $k = 5n$.

6. Using (5) on (2) we have $a = 14(5n) + b = 70n + b$. Therefore by definition of mod, $a \equiv b \ (mod\ 70)$. □

6 Problem 6 (Euler's function)

Let ϕ be Euler's function.

6.1 (a)

What is the value of $\phi(2)$?

Proof. For primes p, we have $\phi(p) = p - 1$, so $\phi(2) = 1$. □

6.2 (b)

What are three nonnegative integers $k > 1$ such that $\phi(k) = 2$?

Proof. $\phi(3) = 3 - 1 = 2$.

ϕ is multiplicative: $\phi(ab) = \phi(a)\phi(b)$.

So $\phi(6) = \phi(2)\phi(3) = (2-1)(3-1) = 2$.

For prime powers p^k we have $\phi(p^k) = p^k - p^{k-1}$.

So $\phi(4) = 4 - 2 = 2$.

So 3,4,6 are three nonnegative integers $k > 1$ such that $\phi(k) = 2$. □

6.3 (c)

Prove that $\phi(k)$ is even for $k > 2$.

Hint: Consider whether k has an odd prime factor or not.

Proof. 1. By the Fundamental Theorem of Arithmetic, k can be uniquely decomposed into its prime factorization

$$k = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$$

for some primes $p_1, \ldots, p_n$ and positive integers $k_1, \ldots, k_n$.

2. By the properties of the ϕ function (multiplicativity, and the formulas for prime powers) we have

$$\begin{aligned} \phi(k) &= \phi(p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}) \\ &= \phi(p_1^{k_1}) \cdot \ldots \cdot \phi(p_n^{k_n}) \\ &= (p_1^{k_1} - p_1^{k_1-1}) \cdot \ldots \cdot (p_n^{k_n} - p_n^{k_n-1}) \\ &= p_1^{k_1-1}(p_1 - 1) \cdot \ldots \cdot p_n^{k_n-1}(p_n - 1) \end{aligned}$$

So, if at least one of these factors $p_i^{k_i-1}(p_i - 1)$ is even, then $\phi(k)$ is even,

3. Case 1: at least one of the $p_1, \ldots, p_n$, say p_i, is odd.

Then $p_i - 1$ is even, so by (2) $\phi(k)$ is even.

4. Case 2: all $p_1, \ldots, p_n$ are even.

In other words, $n = 1$, the only prime in the factorization of k is $p_1 = 2$, and k is a power of 2. Since $k > 2$, $k_1 > 1$. In this case

$$\phi(k) = 2^{k_1-1}(2 - 1) = 2^{k_1-1}$$

is even (because $k_1 - 1 > 0$). $\square$