2020 Mathematical Proof Portfolio

Daniel Kruze

IUPUI Mathematics Department

Prof. Daniel Ramras

MATH-30000: Logic and Foundations/Algebra

December 8, 2020

<u>HW3-#1:</u> (10 Points)

i) Determine the truth value of each of the following statements if the universe is the set $\mathbb{Z}$ of all integers. If true, prove it. If false, write out the negation and prove that the negation is true.

a) $\forall n, \exists m$ such that $(n + m < 10)$, where $n, m \in \mathbb{Z}$.

Since $n, m \in \mathbb{Z}$, $n, m \in \{-\infty, \ldots -1, 0, 1, \ldots \infty\}$, leaving us with two cases:

1) If $n = 10$, then $10 + m < 10$ for the statement to be true. So, if we let $m = -1$, then $10 + m < 10$ is true, because $10 + (-1)$ is 9, and $9 < 10$.

2) If $n \neq 10$, then $n < 10$ or $n > 10$.

2.1) For $n < 10$, let $m = 0$. Here, $n + m = n + 0 = n < 10$. $\therefore n + m < 10$.

2.2) For $n > 10$, $n = (10 + k)$, where $k \in \{1, 2, 3, \ldots \infty\}$. Here, let $m = (-10 - k)$.

$\therefore n + m \in \{(11 + (-11)), (12 + (-12)), \ldots\} = 0 < 10$. $\therefore n + m < 10$.

So, for all n, there does exist m such that $n + m < 10$, making the statement true.

b) $\exists n$ such that $\forall m$, $(n + m < 10)$, where $n, m \in \mathbb{Z}$.

Since $n, m \in \mathbb{Z}$, $n, m \in \{-\infty, \ldots -1, 0, 1, \ldots \infty\}$. If we negate the above statement, we get:

$\forall n, \exists m$ such that $(n + m \geq 10)$, where $n, m \in \mathbb{Z}$, for which there are two cases:

1) If $n = 10$, $10 + m \geq 10$. Letting $m = 0$, we have $10 + 0 = 10 \geq 10$. $\therefore n + m \geq 10$.

2) If $n \neq 10$, then $n < 10$ or $n > 10$.

2.1) If $n < 10$, then $n = (10 - k)$, where $k \in \{1, 2, 3, \ldots \infty\}$. Let $m = k$, so $n + m = (10 - k + k) = 10 \geq 10$. $\therefore n + m \geq 10$.

2.2) If $n > 10$, let $m = 0$. $\therefore$ $n + m = n \geq 10$, and $n + m \geq 10$.

So, the negation of the statement is true, meaning that the statement is false.

c) $\exists n, \exists m$ such that $(n^2 + m^2 = 6)$, where $n, m \in \mathbb{Z}$.

Since $6 \in \mathbb{Z}$, $6 = (0 + 6) = (1 + 5) = (2 + 4) = (3 + 3)$. $\pm\sqrt{5}$, $\sqrt{6}$,$\sqrt{2}$,$\sqrt{3}$ are not members of set $\mathbb{Z}$, $\therefore$ $n + m \neq \pm\sqrt{5}$, $\sqrt{6}$,$\sqrt{2}$,$\sqrt{3}$, so $(n^2 + m^2 \neq 6)$ when $n, m \in \mathbb{Z}$.

So, the statement above is false.

d) $\exists n$ such that $\forall m$, $(nm = 0)$, where $n, m \in \mathbb{Z}$.

Since $n, m \in \mathbb{Z}$, $n, m \in \{-\infty,\ldots -1, 0, 1,\ldots\infty\}$. So, if we let $n = 0$, $nm = 0$ for any m.

This is intrinsically true for all integers, where any integer multiplied by 0 becomes 0.

So, for all m, this statement is true.

e) $\forall m$, $(m \neq 0 \rightarrow \exists n$ such that $(mn = 1))$, where $n, m \in \mathbb{Z}$.

If we negate the statement, we get: $\exists m$, $(m = 0 \land \forall n, (mn \neq 1))$.

Since $n, m \in \mathbb{Z}$, $n, m \in \{-\infty,\ldots -1, 0, 1,\ldots\infty\}$. So, if we let $m = 2$, we have three cases:

1) If $n < 0$, $mn = 2k$, where $k \in \{-\infty,\ldots -3, -2, -1\}$, so $mn \neq 1$.

2) If $n > 0$, $mn = 2l$, where $l \in \{1, 2, 3,\ldots\infty\}$, so $mn \neq 1$.

3) If $n = 0$, $mn = 0$, so $mn \neq 1$.

So, the negation of the statement is true in all cases, meaning that the statement itself is false.

ii) In the set $\mathbb{R}$, would item b, c, or e be any different with regards to truth value?

b) **No:** For $n + m < 10$, for only <u>one</u> value of n, n must equal $-\infty$ since m can go onto ∞. Since n cannot be equal to $-\infty$, the statement cannot be true in $\mathbb{R}$.

c) **Yes:** $\pm \sqrt{5}, \sqrt{6}, \sqrt{2}, \sqrt{3} \in \mathbb{R}$, so n, m can both be equal to $\sqrt{3}$. $\therefore$ ($n^2 + m^2 = 6$), because $3 + 3 = 6$. So, there exist $m, n \in \mathbb{R}$ for which the statement is true.

e) **Yes:** $\forall m \in \mathbb{R}$, $m \neq 0$, $n \in \mathbb{R}$ could be set to $(1/m)$, meaning $mn = 1$ always.

<u>HW2-#6:</u> (5 Points)

Prove that if (4n - 4) is not divisible by 8, then n must be even, where n $\in \mathbb{Z}$.

- So, as a statement, this can be read as $\frac{4n - 4}{8} \notin \mathbb{Z} \rightarrow n = 2k$, where $k \in \mathbb{Z}$.
- If we contrapose, we have that $n = (2k + 1)$, where $k \in \mathbb{Z} \rightarrow \frac{4n - 4}{8} \in \mathbb{Z}$.
- By factoring out a 4, we see that $\frac{4n - 4}{8} = \frac{n - 1}{2}$. $\therefore$ $n = (2k + 1)$, where $k \in \mathbb{Z} \rightarrow \frac{n - 1}{2} \in \mathbb{Z}$; From here, we can substitute n in the antecedent for n in the consequent:
  - $n = (2k + 1)$, where $k \in \mathbb{Z} \rightarrow \frac{2k + 1 - 1}{2} \in \mathbb{Z} = k \in \mathbb{Z}$, which is true.
- So, if $n = (2k + 1)$, where $k \in \mathbb{Z}$, then $\frac{4n - 4}{8} \in \mathbb{Z}$, making the statement's contrapositive implication true: $n = (2k + 1)$, where $k \in \mathbb{Z} \rightarrow \frac{4n - 4}{8} \in \mathbb{Z}$.

$\therefore$ The statement itself is true, by nature of contrapositives, and so if (4n – 4) is not divisible by 8, then n must be even, where $n \in \mathbb{Z}$.

<u>HW9-#4:</u> (5 Points)

Prove Theorem 16.7, which states for two functions, f: A→B and g: B→C

- **If both f and g are one-to-one functions, then g∘f is one-to-one as well.**
- **If both f and g are onto functions, then g∘f is onto as well.**

1) If both f and g are one-to-one, then $\forall a_{1,2} \in A$, $f(a_1) = f(a_2) \rightarrow a_1 = a_2$ and

$\forall b_{1,2} \in B$, $g(b_1) = g(b_2) \rightarrow b_1 = b_2$.

i. $g \circ f = g(f(a))$, where $f(a) = b$. Since f is one-to-one, $f(a_1) = b_1 \neq b_2 = f(a_2)$. So, $g(f(a_1))$ can be taken as equivalent to $g(b_1)$, which, since g is also one-to-one, is equal to c_1, and $c_1 \neq c_2 = g(b_2)$, where $c_{1,2} \in C$.

ii. So, $g(b_1) \neq g(b_2)$, meaning $g(f(a_1)) \neq g(f(a_2))$ when $a_1 \neq a_2$. $\therefore a_1 \neq a_2 \rightarrow g(f(a_1)) \neq g(f(a_2))$, and, by contrapositive, $g(f(a_1)) = g(f(a_2))$, $\rightarrow a_1 = a_2$.

So, g∘f is therefore one-to-one.

2) If both f and g are onto, then $\forall a \in A$, $\exists b \in B$ such that $f(a) = b$, and

$\forall b \in B$, $\exists c \in C$ such that $g(b) = c$.

i. $g \circ f = g(f(a))$, where $f(a) = b$. Since f is onto, $g(f(a)) = g(b)$ for all $a \in A$. Since g is also onto, $g(b) = c$ for all $c \in C$.

ii. $\therefore \forall a \in A$, $g(f(a)) = c$. If g∘f is onto, then $\forall a \in A$, $\exists c \in C$ such that $g(f(a)) = c$, which is true.

So, g∘f is therefore onto.

HW5-#2:

8.14) Define the set A: A = $\mathbb{R}\setminus\bigcap_{n\in\mathbb{Z}^+}(\mathbb{R}\setminus\{\mathbf{-n, -n+1}, \dots \mathbf{0}, \dots \mathbf{n-1, n}\})$ **(5 Points)**

- $\bigcap_{n\in\mathbb{Z}^+}(\mathbb{R}\setminus\{-n, -n+1, \dots 0, \dots n-1, n\})$ can be interpreted as a collection of elements:
  - $\{x: \forall n \in \mathbb{Z}^+, x \in \mathbb{R}\setminus\{-n, -n+1, \dots 0, \dots n-1, n\}\}$, which is the set of all elements in $\mathbb{R}$ that are not integers, including zero. Explicitly, the elements of $\bigcap_{n\in\mathbb{Z}^+}(\mathbb{R}\setminus\{-n, -n+1, \dots 0, \dots n-1, n\}$ are non-integer members of $\mathbb{R}$.
- So, $\mathbb{R}\setminus\bigcap_{n\in\mathbb{Z}^+}(\mathbb{R}\setminus\{-n, -n+1, \dots 0, \dots n-1, n\})$ is all elements in $\mathbb{R}$ that are not non-integers, or all elements that are integers.
  - It can be interpreted symbolically as:
    $(x \in \mathbb{R}) \wedge (x \notin \bigcap_{n\in\mathbb{Z}^+}(\mathbb{R}\setminus\{-n, -n+1, \dots 0, \dots n-1, n\}))$
- So, the set A contains all elements in $\mathbb{R}$ such that those elements are integers, so $\{x: x \in \mathbb{Z}\} = \{x: x \in A\}$, meaning that $A = \mathbb{Z}$**.**

Therefore, set A can be defined as $\mathbb{Z}$, the set of all integers $\{-\infty, \dots -1, 0, 1, \dots \infty\}$.

HW8-#2: **(5 Points)**

What integers have a multiplicative inverse modulo 12?

- To rewrite, this problem asks: For $a \in \mathbb{Z}_{12}$, for which a does $\exists a^{-1}$ such that $a(a^{-1}) = 1\text{mod}12$, where $1\text{mod}12 \equiv 12k + 1$, where $k \in \mathbb{Z}$**.**
  - $\mathbb{Z}_{12}$ in this case represents the ring of equivalence classes on $\mathbb{Z}$, up to 12;
    $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

- If a = 1, $a^{-1} = 1$, so $a(a^{-1}) = 1 \bmod 12$. ∴ 1 has an inverse modulo 12.
- If a = 5, $a^{-1} = 5$, so $a(a^{-1}) = 25 \equiv 1 \bmod 12$. ∴ 5 has an inverse modulo 12.
- If a = 7, $a^{-1} = 7$, so $a(a^{-1}) = 49 \equiv 1 \bmod 12$. ∴ 7 has an inverse modulo 12.
- If a = 11, $a^{-1} = 11$, so $a(a^{-1}) = 121 \equiv 1 \bmod 12$. ∴ 11 has an inverse modulo 12.

So, the integers with multiplicative inverses modulo 12 are all integers that are relatively prime with 12—meaning that gcd(12, a) = 1 for $a \in \mathbb{Z}$ —and, by extension, all integers not in $\mathbb{Z}_{12}$ equivalent modulo 12 to a value with an inverse in $\mathbb{Z}_{12}$ also have inverses modulo 12. (Here, "gcd" is shorthand for "greatest common divisor.")

- For example, $23 \bmod 12 \equiv 11 \bmod 12$, ∴ 23 has a multiplicative inverse—11—modulo 12.

Therefore, in general, <u>all</u> integers $\{x: x \in \mathbb{Z}, \gcd(12, x) = 1\}$ have multiplicative inverses modulo 12.

<u>HW8-#5:</u> (5 points)

F: $\mathbb{R} \setminus \{3/7\}$ is defined by: $F(x) = \frac{x + 2}{7x - 3}$. What is the range of function F?

- Consider what this function states:
  - $\forall x, y \in \mathbb{R}$, $y = \frac{x + 2}{7x - 3}$ if and only if $x = \frac{-3y - 2}{1 - 7y}$.
  - This algebraic manipulation is as follows:

    1) $y(7x - 3) = x + 2$

    2) $7xy - 3y = x + 2$

    3) $x - 7xy = -3y - 2$

4) $x(1 - 7y) = -3y - 2$, $\therefore$ $x = \frac{-3y - 2}{1 - 7y}$

- In other terms, this means that $y(7x - 3) = x + 2$ if and only if $x(1 - 7y) = -3y - 2$.
  - So, using this, we can substitute into our original conditional statement:

    $x = \frac{-3y - 2}{1 - 7y}$ if and only if $x(1 - 7y) = -3y - 2$.

  - $\therefore$ when $y = 1/7$, $x(1 - 7y) \neq -3y - 2$, so $y = 1/7$ is not in the range of F.
- However, what about when $y \neq 1/7$?
  - When $y \neq 1/7$, $x = \frac{-3y - 2}{1 - 7y} \in \mathbb{R}$, and $x(1 - 7y) = -3y - 2$, meaning

    $x = \frac{-3y - 2}{1 - 7y}$ if and only if $x(1 - 7y) = -3y - 2$ is satisfied.

  - So, $y \neq 1/7$ is in the range of F, meaning that $\{y: y \in \mathbb{R}, y \neq 1/7\}$ is the range of F.
- So, the range of function F can be taken as $\mathbb{R}\backslash\{1/7\}$.
- Check by seeing if $x \in \mathbb{R}\backslash\{3/7\}$ when $y = 1/7$:

  1) $1/7 = \frac{x + 2}{7x - 3}$

  2) $\frac{7x + 3}{7} = x + 2$

  3) $x - 3/7 = x + 2$

  4) $x = x + 17/7$; this equation has no real solution.

  - $x \notin \mathbb{R}\backslash\{3/7\}$ when $y = 1/7$, so $y = 1/7$ cannot be in the range of F.

So, the range of F: $\mathbb{R}\backslash\{3/7\}$is $\mathbb{R}\backslash\{1/7\}$.

HW4-#1: (5 Points)

A function F: $\mathbb{R} \to \mathbb{R}$ is defined to be increasing if and only if it satisfies:

$\forall x_1 \in \mathbb{R}, \forall x_2 \in \mathbb{R}, (x_1 < x_2 \to F(x_1) < F(x_2))$.

a) **Negate the definition above.**
   - $\exists x_1 \in \mathbb{R}, \exists x_2 \in \mathbb{R}, (x_1 < x_2 \land F(x_1) \geq F(x_2))$.

b) **Prove that F(x) is not increasing when $F(x) = x^2$.**
   - Check: Does F(x) satisfy the negation above? If so, then F(x) is not increasing.
     i. $\exists x_1 \in \mathbb{R}, \exists x_2 \in \mathbb{R}, (x_1 < x_2 \land x_1^2 \geq x_2^2)$?

     ii. Let $x_1 = -1$, $x_2 = 1$; $-1, 1 \in \mathbb{R}$

     iii. $x_1^2 = 1$, $x_2^2 = 1$, so $(-1 < 1 \land 1 \geq 1)$, $\therefore$ condition **i)** is satisfied.
   - So, there exist two values for which the function $F(x) = x^2$ satisfies the negation of the definition of an increasing function. Therefore, the function F is not increasing.

HW7-#2: (5 Points)

a) **Prove that for $m, n \in \mathbb{Z}$, and $m \neq 0$, and $\forall k \in \mathbb{Z}^+$, gcd(mk, nk) = k(gcd(m, n))**

   1) Recall that for any $m, n \in \mathbb{Z}$, where $m, n \neq 0$, $\exists x, y \in \mathbb{Z}$ such that

   $xm + yn = \gcd(m, n)$.

   2) Use this to rewrite the claim: $\gcd(mk, nk) = k(\gcd(m, n))$ can be written as

   $kxm + kyn = k(xm + yn)$

   which is true for all k, x, y, m, and n by the distributive law of multiplication.

∴ the claim is true for all m, n, and k, so gcd(mk, nk) = k(gcd(m, n)).

3) Note that this is true when both $m, n \neq 0$. Since $m \neq 0$, and the gcd(m, n) is d, where d is an integer that divides both m, n, then $n \neq 0$ when $m \neq 0$. This is because there does <u>not</u> exist any integer d that divides both an integer m and 0.

b) Prove that d = gcd(m, n) → d divides gcd(m + kd, n + ld), where $k, l \in \mathbb{Z}$.

1) If d = gcd(m, n), then m, n must be multiples of d, and can be rewritten as such:

m = wd, n = zd, where $w, z \in \mathbb{Z}$.

2) So, gcd(m + kd, n + ld) = gcd(wd + kd, zd + ld) = gcd(d(w + k), d(z + l)).

3) Since w, z, k, and l are integers, their sums are also integers, meaning gcd(d(w + k), d(z + l)) is the greatest common divisor of two multiples of d, meaning gcd(d(w + k), d(z + l)) = id, $i \in \mathbb{Z}$.

4) Since id is a multiple of d, it follows that d divides id when d = gcd(m, n).

∴ d = gcd(m, n) → d divides gcd(m + kd, n + ld).

<u>HW10-#1:</u> (5 Points)

Prove that if $n \in \mathbb{Z}^+$, and $r \in \mathbb{R}$ such that $r \neq 1$, then $\sum_{k=0}^{n-1} r^k = \frac{1 - r^n}{1 - r}$ holds true.

- Here, let $p(n) \coloneqq \sum_{k=0}^{n-1} r^k = \frac{1 - r^n}{1 - r}$, which can be interpreted as

  $r^0 + r^1 + r^2 + \ldots r^{n-1} = \frac{1 - r^n}{1 - r}$.

- Let $p(n_0) = p(1) \coloneqq r^0 = \frac{1 - r}{1 - r}$, which is true for all $r \in \mathbb{R}\backslash\{1\}$.

- Now, assume that p(n) holds true for all subsequent values of n, where $n \geq n_0$.

  From here, we can substitute n + 1 for n in our equation p(n):

  $r^0 + r^1 + r^2 + \ldots r^n = \frac{1 - r(r^n)}{1 - r}$

- Now, for this p(n + 1), let $p(n_0 + 1) = p(2) \coloneqq r^0 + r^1 = \frac{1 - r^2}{1 - r}$
  - $p(2) \coloneqq 1 + r = \frac{(1 - r)(1 + r)}{1 - r}$ which is true for all $r \in \mathbb{R} \setminus \{1\}$.
  - So, $p(n_0) \rightarrow p(n_0 + 1)$, and $p(n_0)$, $p(n_0 + 1)$ are true.
- So, if we assume that p(n) is true for all $n > n_0$ as well, then we can induce that

  $p(n) \rightarrow p(n + 1)$ where $n \geq n_0$, $n \in \mathbb{N}$ ($\mathbb{N}$ being the set of natural numbers, $\{1, 2, 3, \ldots \infty\}$).
- Therefore, if $n \in \mathbb{Z}^+$, and $r \in \mathbb{R} \setminus \{1\}$, then $\sum_{k=0}^{n-1} r^k = \frac{1 - r^n}{1 - r}$.