question	1	2	3	4	5	Total
score						

MATH213 First Midterm Solutions
Fall 2022

NAME: ______________________

Instructor: M. Zhang

Please answer all first *four* questions (question 5 is optional).

- You are allowed one double-sided cheat sheet.
- Show all work for full credit.
- Each is of equal worth (sub-problems within a problem are of equal worth).
- No calculators are permitted.

Good luck!

Answer:

1. (25 points)

   (a) Suppose P and Q are predicates, and x and y are variables. Suppose all quantifiers we considered have the same nonempty domain. Prove or disprove that $\forall x(P(x) \to Q(x))$ and $\forall x P(x) \to \forall x Q(x)$ are logically equivalent.

   (b) Prove or disprove that, for each real number x, x is rational if and only if $x/2$ is rational.

Solutions: (a) They are **NOT equivalent**. For example, let $P(x)$ be a propositional

function such that $P(x)$ is true for some x in the domain and false for the rest. Let $Q(x)$ be a propositional function that is always false for all x in the domain. Then, there exists an x_0 in the domain such that $P(x_0)$ is true and $Q(x_0)$ is false, i.e., $P(x_0) \to Q(x_0)$ is false. Thus, $\forall x(P(x) \to Q(x))$ is false. On the other hand, there exists an x_1 in the domain such that $P(x_1)$ is false. Thus, $\forall x P(x)$ is false, so $\forall x P(x) \to \forall x Q(x)$ is true.

(b)

- If x is rational, then there exist integers m_1 and n_1 such that $x = m_1/n_1$. We have $\frac{x}{2} = \frac{m_1}{2n_1}$, which is also rational.
- If $x/2 = m_2/n_2$, then we have $x = \frac{2m_2}{n_1}$, which is also rational.

2. (30 points)

   (a) Consider sets A and B. Prove or disprove the following:

   – $\mathcal{P}(A \times B) = \mathcal{P}(B \times A)$.

   – $(A \oplus B) \oplus B = A$, where $A \oplus B$ denotes the set containing those elements in either A or B, but not both.

   (b) Give an example of a function from $\mathbf{N}$ to $\mathbf{N}$ that is

   – one-to-one but not onto.

   – onto but not one-to-one.

Solution:

(a) – This is **false**. Consider the following counterexample with set $A = \{1\}$ and set $B = \{2\}$. We have $A \times B = \{(1, 2)\}$ and $B \times A = \{(2, 1)\}$. We have

$$\mathcal{P}(B \times A) = \{\{(1, 2)\}, \emptyset\} \neq \mathcal{P}(A \times B) = \{\{(2, 1)\}, \emptyset\}.$$

– This is **true**. Let p be $x \in A$ and q be $x \in B$. Consider the following truth table:

p	q	$p \oplus q$	$(p \oplus q) \oplus q$
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

It implies that $p = (p \oplus q) \oplus q$.
Note that $A = \{x | x \in A\}$ and $(A \oplus B) \oplus B = \{x | x \in (A \oplus B) \oplus B\}$. We see that $A = (A \oplus B) \oplus B$.

(b) – An example: $f(x) = 2x$

– An example: $f(x) = \begin{cases} 1, & \text{if } \ x = 0 \\ x - 1, & \text{otherwise} \end{cases}$.

3. (20 points) Let $f_1 : \mathbf{Z}^+ \to \mathbf{R}^+$, and $f_2 : \mathbf{Z}^+ \to \mathbf{R}^+$. Let $g : \mathbf{Z}^+ \to \mathbf{R}$, and suppose $f_1(x)$ and $f_2(x)$ are both $\Theta(g(x))$.

   (a) Prove or disprove that $(f_1 - f_2)(x)$ is $\Theta(g(x))$.

   (b) Prove or disprove that $(f_1 f_2)(x)$ is $\Theta(g^2(x))$, where $g^2(x) = (g(x))^2$.

Solution:

(a) This is false. Consider a counterexample. Let $f_1(x) = x^2 + 2$, $f_2(x) = x^2 + 1$, and $g(x) = x^2$. Thus, $f_1(x)$ and $f_2(x)$ are both $\Theta(g(x))$. Note that $(f_1 - f_2)(x) = 1$, which is not $\Theta(g(x))$.

(b) It is true that $(f_1 f_2)(x)$ is $\Theta(g^2(x))$. By the definition of Θ, since $f_1(x)$ and $f_2(x)$ are both $\Theta(g(x))$, there exist real numbers C_1, C_1', C_2, and C_2' and positive real numbers k_1 and k_2 such that

$$C_1|g(x)| \leq |f_1(x)| \leq C_1'|g(x)|, \; x > k_1,$$

$$C_2|g(x)| \leq |f_2(x)| \leq C_2'|g(x)|, \; x > k_2.$$

Thus, let $k = \max\{k_1, k_2\}$, $C = C_1C_2$, and $C' = C_1'C_2'$. Then, since $f_1(x) > 0$ and $f_2(x) > 0$, we have

$$C(|g(x)|)^2 \leq |(f_1 f_2)(x)| \leq C'(|g(x)|)^2, \; x > k.$$

That is, $C|(g(x))^2| \leq |(f_1 f_2)(x)| \leq |C'(g(x))^2|, \; x > k$. Thus, $(f_1 f_2)(x)$ is $\Theta(g^2(x))$.

4. (25 points)

   (a) Convert $(11110111)_2$ to an octal expansion.

   (b) Convert $(101)_{10}$ to a binary expansion.

   (c) Compute $\gcd(210, 1638)$ without calculator and explain your answer.

   Solution:

   (a) $(367)_8$

   (b) $(1100101)_2$

   (c) Since

$$\begin{aligned} 1638 &= 210 \times 7 + 168 \\ 210 &= 168 \times 1 + 42 \\ 168 &= 42 \times 4 + 0 \end{aligned}$$

   Therefore, we have $\gcd(210, 1638) = \gcd(168, 210) = 42$.

5. (Bonus 25 points) Suppose that a is not divisible by the prime p.

   (a) Show that no two of the integers $1 \cdot a, 2 \cdot a, ..., (p-1)a$ are congruent modulo p.

   (b) Use the result in (a), show that

$$(p-1)! \equiv a^{(p-1)}(p-1)! (\textbf{mod}\ p).$$

Solution: The proofs in this question are part of the proof of Fermat's Little Theorem. Please check the following link for more details:

`https://primes.utm.edu/notes/proofs/FermatsLittleTheorem.html`