Math 325K Fall 2018
Midterm Exam #1 Solutions

Bo Lin

1. (8 pts) True/False: each of the following arguments is either true or false and please mark your choice. You get 2 pts for each correct choice, 1 pt for **NOT** answering each question, and 0 pt for each incorrect/multiple choice. You **do not** need to justify your answer.

(1) The elements in a set are unordered.

Solution. $\boxed{True}$. *A set is uniquely determined by its elements and for each element, it either belongs to the set or not, so the order does not matter.*

(2) The relation $C = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y^2\}$ is a function from $\mathbb{R}$ to $\mathbb{R}$.

Solution. $\boxed{False}$. *The domain and the co-domain of C are both $\mathbb{R}$. When $x = 1$, $y^2 = 1$, so $y = \pm 1$. Hence both $(1, 1), (1, -1) \in C$, by definition of a function, C is not a function.*

(3) The converse and the inverse of the same conditional statement p are always logically equivalent.

Solution. $\boxed{True}$. *Suppose p is of the form $q \to r$. The converse of p is $r \to q$ and the inverse of p is $\sim q \to \sim r$. They are the contrapositive of each other and thus they are logically equivalent.*

(4) When testing whether an argument form is valid, if the corresponding truth table has no critical row, then the argument form is invalid.

Solution. $\boxed{False}$. *By definition, an argument form is valid if and only if in all critical rows of the truth table, the conclusion is true. So if there is no critical row at all, this property automatically holds and thus the argument form is valid.*

2. (8 pts) Multiple choices: there is **exactly one** correct answer for each question. You get 4 pts for each correct choice, 1 pt for **NOT** answering each question, and 0 pt for each incorrect/multiple choice. You **do not** need to justify your answer.

(1) Which of the following statements is **NOT** logically equivalent to the negation of the statement "some spicy tacos are vegetarian"?

(a) All vegetarian tacos are not spicy.

(b) All non-spicy tacos are vegetarian.

(c) For any taco t, if t is spicy, then t is not vegetarian.

(d) For any taco t, t is not spicy or not vegetarian.

Solution. *The answer is* $\boxed{(b)}$. *Let the domain D be the set of all tacos. And predicate $S(x)$ be "x is spicy", predicate $V(x)$ be "x is vegetarian." The original statement is "there exists an $x \in D$ such that $S(x)$ and $V(x)$ are both true." Then the negation would be "for all $x \in D$, $S(x)$ or $V(x)$ is false.", which is exactly (c) and (d). As for (a), it is "for all $x \in D, V(x) \to {\sim}S(x)$." Since $V(x) \to {\sim}S(x)$ is logically equivalent to "${\sim}V(x) \vee {\sim}S(x)$," it is also logically equivalent to the negation. And (b) is "for all $x \in D, {\sim}S(x) \to V(x)$." And ${\sim}S(x) \to V(x)$ is logically equivalent to $S(x) \vee V(x)$, which is not the negation.*

(2) Which of the following arguments is invalid?

(a) If I drank coffee last night, I could not fall asleep; I did fall asleep last night; $\therefore$ I didn't drink coffee last night.

(b) If Jane listens to music on the bus, then she is happy; if Jane reads a book on the bus, then she is happy; Jane either listens to music or reads a book on the bus; $\therefore$ Jane is happy.

(c) If John is at least 16 years old, then he can have a driver's license; If one has a driver's license, then he/she has a photo ID; John is 15 years old; $\therefore$ John does not have a photo ID.

(d) Any Canadian citizen can travel in the Schengen area without a visa for up to 90 days; Italy is a country in the Schengen area; Alice is a Canadian citizen; $\therefore$ Alice can travel in Italy without a visa for up to 90 days.

Solution. *The answer is* $\boxed{(c)}$. *(a) is proof by contraposition; (b) is proof by division into cases; (d) is proof by generalizing from general particular twice. As for (c), it is an inverse error.*

3. (4 pts) Prove that the statement form

$$p \to (q \to p)$$

is a tautology.

Proof. Method 1: we write the following truth table

p	q	$q \to p$	$p \to (q \to p)$
T	T	T	T
T	F	T	T
F	T	F	T
F	T	T	T

Since no matter what are the truth values of the statement variables p and q, the statement $p \to (q \to p)$ is always true, it is a tautology.

Method 2: note that $q \to p \equiv {\sim}q \vee p$. So

$$p \to (q \to p) \equiv {\sim}p \vee (q \to p) \equiv {\sim}p \vee {\sim}q \vee p.$$

Since ${\sim}p \vee p$ is a tautology, so is ${\sim}p \vee {\sim}q \vee p$. □

4. (5 pts) The Exclusive OR (XOR for short) is another binary logical connective, denoted by the symbol $\oplus$, its truth table is as follows:

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Question: Is the statement form $(p \oplus q) \oplus r$ logically equivalent to the statement form $p \oplus (q \oplus r)$? Justify your answer.

Solution. *The answer is* $\boxed{yes}$. *For a proof, there are two methods.*
Method 1: we can write the following truth table:

p	q	r	$p \oplus q$	$q \oplus r$	$(p \oplus q) \oplus r$	$p \oplus (q \oplus r)$
T	T	T	F	F	T	T
T	T	F	F	T	F	F
T	F	T	T	T	F	F
T	F	F	T	F	T	T
F	T	T	T	F	F	F
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

Since the two statements always have the same truth value, they are logically equivalent.

Method 2: This is an alternative proof that utilizes the property of congruence modulo 2. Let f be the function $\{T, F\} \to \{0, 1\}$ such that $f(T) = 1$ and $f(F) = 0$. Then for any statements p, q, we have

$$f(p \oplus q) = (f(p) + f(q)) \ \ mod\ 2.$$

Then

$$\begin{aligned} f((p \oplus q) \oplus r) &= (f(p \oplus q) + f(r)) \;\; mod\ 2 \\ &= [(f(p) + f(q)) \;\; mod\ 2 + f(r)] \;\; mod\ 2 \\ &= [f(p) + f(q) + f(r)] \;\; mod\ 2. \end{aligned}$$

Similarly, we have

$$f(p \oplus (q \oplus r)) = f((q \oplus r) \oplus p) = [f(q) + f(r) + f(p)] \;\; mod\ 2.$$

So $(p \oplus q) \oplus r$ and $p \oplus (q \oplus r)$ are always mapped to the same value by f, then their truth values must be equal too. So they are logically equivalent.

5. (4 pts) Prove that for any integers a and b, if 2 divides $a - b$, then 2 divides $a^2 + b^2$.

Proof. Let a, b be two arbitrary integers such that $2 \mid (a - b)$. Then there is an integer k such that $a - b = 2k$, and thus $a = b + 2k$. Then

$$a^2 + b^2 = (b + 2k)^2 + b^2 = 2b^2 + 4bk + 4k^2 = 2 \cdot (b^2 + 2bk + 2k^2).$$

Since both b and k are integers, so is $b^2 + 2bk + 2k^2$. By definition, 2 divides $2 \cdot (b^2 + 2bk + 2k^2)$, which is exactly $a^2 + b^2$. □

6. (6 pts) Let $D(x, y)$ be the binary predicate "x divides y". Rewrite the statement

$$\exists x \in \mathbb{N} \text{ such that } (x > 1) \wedge \left(\forall y \in \mathbb{N}, D(x, y^2) \rightarrow D(x, y)\right).$$

in an English sentence, and determine whether it is true or false. Justify your answer.

Solution. *The statement is "there exists an integer x greater than 1 such that for any positive integer y, if x divides y^2, then x divides y". It is $\boxed{\textit{true}}$. Since it is an existential statement, one example suffices to justify it. We show that $x = 2$ is such an example. When $x = 2$, the statement becomes "for any positive integer y, if y^2 is even, then y is also even," which we have already shown in a lecture, using proof by contradiction.*

7. (5 pts) Let $n > 1$ be a composite number. Prove that there exists at least one prime divisor of n that is less than or equals to $\sqrt{n}$.

Proof. We prove by contradiction. Suppose $n > 1$ is a composite number whose prime divisors are all strictly greater than $\sqrt{n}$. Since n is composite, by definition there are two integers a and b such that $ab = n$ and $a, b > 1$. By Theorem 4.3.4, every integer greater than 1 has at least one prime divisor. So there exists a prime number p that is a divisor of a, and there exists a prime number q that is a divisor of b. By our assumption, both p, q are greater than $\sqrt{n}$, then $pq > (\sqrt{n})^2 = n$. Since $p \mid a$, by Theorem 4.3.1 we have $p \leq a$; since $q \mid b$, for the same reason we have $q \leq b$. Now we have

$$n = ab \geq pq > n,$$

a contradiction! So our assumption is false and we are done. □

8. Extra Problem. (6 pts)

(1) (2 pt) Prove that for any two integers m and n, if $m \bmod 4 = n \bmod 4 = 1$, then $mn \bmod 4 = 1$.

(2) (4 pt) Prove that there exist infinitely many prime numbers p such that $p \bmod 4 = 3$. (Hint: proof by contradiction)

Proof. (1) Suppose m and n are two arbitrary integers such that $m \bmod 4 = n \bmod 4 = 1$. By definition, there is an integer k such that $m = 4k + 1$ and there is an integer l such that $n = 4l + 1$. Then

$$mn = (4k + 1)(4l + 1) = 16kl + 4k + 4l + 1 = 4 \cdot (4kl + k + l) + 1.$$

Since k, l are both integers, so is $4kl + k + l$. In addition, integer 1 satisfies $0 \leq 1 < 4$, by definition of div, we have $mn \bmod 4 = 1$.

(2) We prove by contradiction. Suppose there are only finitely many prime number whose remainder is 3 when divided by 4. Let they be

$$3 = q_1 < q_2 < \cdots < q_N,$$

where N is some positive integer. Let

$$M = 2 \cdot q_1 \cdot q_2 \cdot \cdots \cdot q_N + 1.$$

Since all q_i's are odd, so is their product, and thus the product doubled is not a multiple of 4. Then $M \bmod 4 = 2 + 1 = 3$. Note that for each $1 \leq i \leq N$, $M - 1$ is a multiple of q_i, by Proposition 4.6.3, M is not a multiple of q_i. Since M is odd, 2 is neither a divisor of M. Then all prime divisors of M must have remainder 1 when divided by 4. By the unique factorization theorem, since $M > 1$, M is the product of finitely many prime divisors. By (1), $M \bmod 4 = 1$, a contradiction! So our assumption is false and we are done.

(Remark: alternatively, since the square of an odd number is of the form $4K+1$, we can also choose

$$M' = q_1^2 \cdot q_2^2 \cdot \cdots \cdot q_N^2 + 2.$$

As long as $M \bmod 4 = 3$ and M is not divisible by any q_i, we can get a contradiction.) $\square$