HKUST – Department of Computer Science and Engineering

COMP 2711: Discrete Math Tools for Computer Science

Spring 2020 Midterm Examination

Date: Monday, 6 April 2018   Time: 19:00–20:40

Problem 1: [8 pts] Let $Z(x)$, $D(x)$, $F(x)$ and $C(x)$ be the following predicates:

$Z(x)$: "x attended the Zoom meeting of midterm dry run".

$D(x)$: "x gets some marks deducted for the midterm exam".

$F(x)$: "x submitted a file for the midterm dry run".

$C(x)$: "x is cheating".

Express the following statements using quantifiers, logical connectives, and the predicates above, where the domain consists of all students in COMP2711.

(a) Any student absent from the Zoom meeting of midterm dry run gets some marks deducted for the midterm exam.

(b) If a student attended the Zoom meeting of midterm dry run but got some marks deducted for the midterm exam, then he/she must have not submitted a file for the midterm dry run.

(c) Some students were absent from the Zoom meeting of midterm dry run but did not get marks deducted for the midterm exam.

(d) Any student who submitted a file for the midterm dry run but were absent from the Zoom meeting of midterm dry run is considered as cheating.

Answer: (a) $\forall x(\neg Z(x) \to D(x))$.

(b) $\forall x(Z(x) \wedge D(x) \to \neg F(x))$.

(c) $\exists x(\neg Z(x) \wedge \neg D(x))$.

(d) $\forall x(F(x) \wedge \neg Z(x) \to C(x))$.

Problem 2: [10 pts] Determine whether the following two propositions are logically equivalent.

(i) $((\neg p \wedge q) \to (p \vee s)) \vee ((\neg(\neg q \wedge p) \wedge q) \to (s \vee r))$,

(ii) $q \to (p \vee s \vee r)$

If they are, prove it by a series of logical equivalences. If they are not, give a counterexample.

Answer:

$$
\begin{aligned}
&((\neg p \wedge q) \rightarrow (p \vee s)) \vee ((\neg(\neg q \wedge p) \wedge q) \rightarrow (s \vee r)) \\
\equiv\ &((\neg p \wedge q) \rightarrow (p \vee s)) \vee (((q \vee \neg p) \wedge q) \rightarrow (s \vee r)) \\
\equiv\ &((\neg p \wedge q) \rightarrow (p \vee s)) \vee (q \rightarrow (s \vee r)) \\
\equiv\ &(\neg(\neg p \wedge q) \vee (p \vee s)) \vee (\neg q \vee (s \vee r)) \\
\equiv\ &((p \vee \neg q) \vee (p \vee s)) \vee (\neg q \vee (s \vee r)) \\
\equiv\ &\neg q \vee p \vee s \vee r \\
\equiv\ &q \rightarrow (p \vee s \vee r)
\end{aligned}
$$

Problem 3: [12 pts] For each of the following statement, determine it is true or false. Justification is not required. The domain is the set of real numbers.

(a) $\forall x(|x| \cdot x \geq x)$

(b) $\forall x \forall y((x > 2 \wedge y > 2) \rightarrow (xy > x + y))$

(c) $\forall x \exists y(x = 2y + 3)$

(d) $\exists y \forall x(x = 2y + 3)$

(e) $\forall x((x > 1) \rightarrow (x^2 > x)) \leftrightarrow \neg \exists x((x > 1) \rightarrow (x^2 \leq x))$

(f) $\forall x((x > 1) \rightarrow (x^2 > x)) \leftrightarrow \neg \exists x((x > 1) \wedge (x^2 \leq x))$

Answer: (a) False. When $x = -2$, we have $2 \cdot -2 = -4 < -2$.

(b) True. When $y > 2$, $y/(y-1) < 2$. So, $x > y/(y-1)$. This implies $x(y-1) > y$, and thus $xy > x + y$.

(c) True. There is always a $y = (x-3)/2$.

(d) False. For every y, there exists an $x \neq 2y + 3$.

(e) False.

$$
\begin{aligned}
&\neg \exists x((x > 1) \rightarrow (x^2 \leq x)) \\
\equiv\ &\forall x \neg((x > 1) \rightarrow (x^2 \leq x)) \\
\equiv\ &\forall x \neg(\neg(x > 1) \vee (x^2 \leq x)) \\
\equiv\ &\forall x((x > 1) \wedge (x^2 > x))
\end{aligned}
$$

which is false when $x \leq 1$. However, $\forall x((x > 1) \rightarrow (x^2 > x))$ is true.

(f) True.

$$
\begin{aligned}
&\neg \exists x((x > 1) \wedge (x^2 \leq x)) \\
\equiv\ &\forall x \neg((x > 1) \wedge (x^2 \leq x)) \\
\equiv\ &\forall x((x \leq 1) \vee (x^2 > x)) \\
\equiv\ &\forall x((x > 1) \rightarrow (x^2 > x))
\end{aligned}
$$

Problem 4: [10 pts] Recall that we can express unique existence as

$$\exists x(P(x) \wedge \forall y(P(y) \rightarrow x = y)) \tag{1}$$

In many unique existence proofs, instead of proving (1), we prove the following:

$$
\begin{array}{ll}
(2) & \exists x P(x) \\
(3) & \forall x \forall y (P(x) \wedge P(y) \rightarrow x = y)
\end{array}
$$

Your task here is to prove (1) from (2) and (3) using the rules of inference for propositional and predicate logic.

Answer:

$$
\begin{array}{lll}
(4) & P(c) \text{ for some c} & (2), \text{existential instantiation} \\
(5) & \forall y (P(c) \wedge P(y) \rightarrow c = y) & (3), \text{universal instantiation} \\
(6) & \forall y (\neg P(c) \vee \neg P(y) \vee c = y) & (5), \text{equivalence} \\
(7) & \forall y (\neg P(y) \vee c = y) & (4), (6), \text{resolution} \\
(8) & \forall y (P(y) \rightarrow c = y) & (7), \text{equivalence} \\
(9) & \forall y (P(c) \wedge (P(y) \rightarrow c = y)) & (4), (8), \text{conjunction} \\
(10) & \exists x \forall y (P(x) \wedge (P(y) \rightarrow x = y)) & (9), \text{existential generalization} \\
(11) & \exists x (P(x) \wedge \forall y (P(y) \rightarrow x = y)) & (10), \text{null qualification}
\end{array}
$$

Problem 5: [10 pts] Decide if the following sets are countable or uncountable. Let $\mathbf{N}$ be the set of natural numbers. $P(S)$ denotes the power set of S. No need to justify your answers.

(a) $\mathbf{N}^3$

(b) $P(\mathbf{N})$

(c) $P(P(\mathbf{N}))$

(d) The set of all functions from $\mathbf{N}$ to $\mathbf{N}$

(e) The set of all functions from $\{0, 1\}$ to $\mathbf{N}$

Answer: (a) Countable; (b) Uncountable; (c) Uncountable; (d) Uncountable; (e) Countable.

Problem 6: [10 pts] Use the extended Euclid algorithm to find the inverse of 53 (mod 180). Show the steps of the algorithm.

Answer: Calculate $gcd(180, 53)$ using euclidean algorithm.

$180 = 53 \cdot 3 + 21$
$53 = 21 \cdot 2 + 11$
$21 = 11 \cdot 1 + 10$
$11 = 10 \cdot 1 + 1$
$10 = 1 \cdot 10 + 0$
So $gcd(180, 53) = 1$.

Rewriting:
$21 = 180 - 53 \cdot 3$

$11 = 53 - 21 \cdot 2$
$10 = 21 - 11 \cdot 1$
$1 = 11 - 10 \cdot 1$

Substituting:
$1 = 11 - 10 \cdot 1$
$1 = 11 - (21 - 11 \cdot 1) \cdot 1$
$1 = 21 \cdot (-1) + 11 \cdot (2)$
$1 = 21 \cdot (-1) + (53 - 21 \cdot 2) \cdot (2)$
$1 = 53 \cdot (2) + 21 \cdot (-5)$
$1 = 53 \cdot (2) + (180 - 53 \cdot 3) \cdot (-5)$
$1 = 180 \cdot (-5) + 53 \cdot 17$

So 17 is the modular inverse of $53 \pmod{180}$

Problem 7: [10 pts] Solve $10x + 4 \equiv 0 \pmod{23}$.

Answer: Solve $10x \equiv -4 \pmod{23}$

As $gcd(10, 23) = 1$ we can multiply both sides by the inverse of $10 \pmod{23}$. We calculate the inverse of $10 \pmod{23}$ using extended Euclidean algorithm.

$23 = 10 \cdot 2 + 3$
$10 = 3 \cdot 3 + 1$
$3 = 1 \cdot 3 + 0$

Rewriting:
$3 = 23 - 10 \cdot 2$
$1 = 10 - 3 \cdot 3$

Substituting:
$1 = 10 - 3 \cdot 3$
$1 = 10 - (23 - 10 \cdot 2) \cdot 3$
$1 = 23 \cdot (-1) + 10 \cdot 7$
7 is the modular inverse of $10 \pmod{23}$. We multiply both sides by 7.

$10x \equiv -4 \pmod{23} \implies 10x \cdot 10^{-1} \equiv -4 \cdot 10^{-1} \implies x \equiv -4 \cdot 7 \equiv -28 \equiv 18$. $\quad x \equiv 18 \pmod{23}$ is the final answer.

Problem 8: [10 pts] Show that $gcd(21n + 4, 14n + 3) = 1$, for any $n \in \mathbf{N}$.

Proof: Using the Euclid's algorithm, we have $gcd(21n + 4, 14n + 3) = gcd(14n + 3, 7n + 1) = gcd(7n + 1, 1) = 1$.

Problem 9: [10 pts] Solve $3^{5x-2} \equiv 9 \pmod{23}$. The solution is not unique, any solution is acceptable. [Hint: Use Fermat's Little Theorem.]

Answer: Multiplying 3^{-2} (inverse taken with modulo 23) on both sides, we obtain:

$$3^{5x-4} \equiv 1 \pmod{23}.$$

By Fermat's Little Theorem, if $5x - 4$ is a multiple of 22, then this congruence will hold, namely $5x - 4 \equiv 0 \pmod{22}$, i.e.,

$$5x \equiv 4 \pmod{22}.$$

The inverse of 5 is 9 (mod 22), so $x \equiv 4 \cdot 9 \equiv 36 \equiv 14 \pmod{22}$. So $x = 22k + 14$ for any natural number k.

Problem 10: [10 pts] Recall the digital signature scheme based on RSA. Suppose your public key is (n, e) and private key is d, and you want to sign a message $x \in \mathbf{Z}_n$. You release both x and $C = x^d \bmod n$. People can then verify your signature by checking $C^e \bmod n = x$.

However, you should be careful not to just sign any message people give you. Suppose an attacker asks you to sign another message $y = r^e x \bmod n$ where $r \neq 1$ is a number chosen by the attacker, and you sign it (i.e., release $y^d \bmod n$). Then the attacker can forge your signature on x, i,e, compute C without knowing d. Show how the attacker can do this. (This is known as a *chosen-message-attack*.)

Answer: $y^d \equiv (r^e x)^d \equiv r^{ed} \cdot x^d \equiv r \cdot x^d \pmod{n}$.

So the attacker can just find r^{-1} (in $\mathbf{Z}_n$), and then compute $y^d \cdot r^{-1} \equiv x^d \equiv C \pmod{n}$.

Bonus Problem: [10 pts] A *quasi-square* number $n \in \mathbf{N}$ is one that is divisible by a square number. For example, 24 is a quasi-square number because it is divisible by $4 = 2^2$, while 15 is not a quasi-square number.

Prove that for any $k \in \mathbf{N}$, there exist k consecutive numbers all of which are quasi-square numbers. [Hint: Use the Chinese Remainder Theorem.]

Proof: We give a constructive proof. Let p_i be the ith prime number. We know that $gcd(p_i^2, p_j^2) = 1$ for $i \neq j$. Consider the following system of linear congruences:

$x \equiv -1 \pmod{p_1^2}$
$x \equiv -2 \pmod{p_2^2}$
$\ldots$
$x \equiv -k \pmod{p_k^2}$.

Based on the Chinese Remainder Theorem, there is a solution $x_0 \in \mathbf{Z}_n$ to this system for $n = p_1^2 \ldots p_k^2$. We know that

$p_1^2 \mid x_0 + 1$
$p_2^2 \mid x_0 + 2$
$\ldots$
$p_k^2 \mid x_0 + k$
So $x_0 + 1, \ldots, x_0 + k$ are all quasi-square numbers.