HKUST – Department of Computer Science and Engineering

COMP 2711: Discrete Math Tools for Computer Science

Spring 2019 Midterm Examination

Date: Friday, 22 March 2019 Time: 19:00–21:00

Name: ________________ Student ID: ________________

Email: ________________ Lecture: ________________

Instructions

- This is a closed book exam. It consists of 17 pages and 13 questions.
- Please write your name, student ID, email, lecture section in the space provided at the top of this page.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.

Questions	1	2	3	4	5	6	7	8	9	10	11	12	Total	Bonus
Points	8	12	6	8	6	6	8	8	6	12	12	8	100	10
Score														

Student ID: ______________

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: ______________________________

Student's Signature: _________________________

Student ID: ____________

Problem 1: [8 pts] Let c, d, r, and w be the propositiions

c: "It is cold"

d: "It is dry"

r: "It is rainy"

w: "It is windy"

Write the following propositions using c, d, r and w and the Boolean connectives.

(a) It is neither cold nor dry.

(b) It is rainy if it is not cold.

(c) To be windy it is necessary that it be cold.

(d) It is rainy only if it is windy and cold.

Answer: (a) $\neg c \wedge \neg d$.

(b) $\neg c \rightarrow r$.

(c) $w \rightarrow c$.

(d) $r \rightarrow (w \wedge c)$.

Grading Scheme: 2,2,2,2

Problem 2: [12 pts] Let $P(x)$ be the statement "x is even" and $Q(x)$ be the statement "x is an integer". Express each of the following statements using predicates, quantifiers, logical connectives, and mathematical operators where the domain is all real numbers.

(a) Some real numbers are not positive.

(b) Every integer is even.

(c) Some integers are odd.

(d) If $x < y$, then x is not equal to y.

(e) There is no largest real number.

Answer: (a) $\exists x \ (x \leq 0)$.

(b) $\forall x \ (Q(x) \rightarrow P(x))$.

(c) $\exists x \ (Q(x) \wedge \neg P(x))$.

(d) $\forall x \forall y \ ((x < y) \rightarrow (x \neq y))$.

(e) $\forall x \exists y \ (y > x)$.

Grading Scheme: 2,2,2,3,3

Problem 3: [6 pts] For each of the following propositions, determine whether the proposition is a tautology. If yes, prove it using propositional equivalence and the laws of logic. If not, give a counterexample which consists of the truth values of the propositions under the setting.

(a) $((p \to q) \wedge \neg p) \to \neg q$

(b) $((p \to \neg q) \wedge q) \to \neg p$

Answer: (a) No. Set $p = F$ and $q = T$. We have $((F \to T) \wedge T) \to F \equiv T \to F \equiv F$.

(b) Yes.

$$\begin{aligned}
&((p \to \neg q) \wedge q) \to \neg p \\
\equiv\ &(\neg p \vee \neg q) \wedge q) \to \neg p \\
\equiv\ &(\neg p \wedge q) \to \neg p \\
\equiv\ &\neg(\neg p \wedge q) \vee \neg p \\
\equiv\ &(p \vee \neg q) \vee \neg p \\
\equiv\ &T
\end{aligned}$$

Grading Scheme 3,3

Problem 4: [8 pts] Consider the following argument:

Premise 1: $\exists x\ P(x)$.
Premise 2: $\forall x\ (P(x) \to Q(x))$.
Premise 3: $\forall x\ (P(x) \to R(x))$.
Conclusion: $\exists x\ (Q(x) \land R(x))$.

Show that the argument is valid. Number your steps and refer to those numbers in the reason you give for each step, but it is not necessary to give the name of the inference rule.

Answer:

Step	**Reason**
1. $\exists x\ P(x)$	Hypothesis
2. $P(c)$	(1), Existential instantiation
3. $\forall x\ (P(x) \to Q(x))$	Hypothesis
4. $P(c) \to Q(c)$	(3), Universal instantiation
5. $\forall x\ (P(x) \to R(x))$	Hypothesis
6. $P(c) \to R(c)$	(5), Universal instantiation
7. $Q(c)$	(2) and (4), Modus ponens
8. $R(c)$	(2) and (6), Modus ponens
9. $Q(c) \land R(c)$	(7) and (8), Conjunction
10. $\exists x\ (Q(x) \land R(w))$	(9), Existential generalization

Student ID: ____________

Problem 5: [6 pts] Express the negations of $\forall x\ (P(x) \land \exists y \forall z\ (Q(x,y) \rightarrow R(y,z)))$ so that all negation symbols immediately precede predicates.

Answer:

$$\begin{aligned}
&\neg\forall x\ (P(x) \land \exists y \forall z\ (Q(x,y) \rightarrow R(y,z))) \\
\equiv\ &\exists x\ \neg(P(x) \land \exists y \forall z\ (Q(x,y) \rightarrow R(y,z))) \\
\equiv\ &\exists x\ (\neg P(x) \lor \neg\exists y \forall z\ (Q(x,y) \rightarrow R(y,z))) \\
\equiv\ &\exists x\ (\neg P(x) \lor \forall y \neg\forall z\ (Q(x,y) \rightarrow R(y,z))) \\
\equiv\ &\exists x\ (\neg P(x) \lor \forall y \exists z\ \neg(Q(x,y) \rightarrow R(y,z))) \\
\equiv\ &\exists x\ (\neg P(x) \lor \forall y \exists z\ (Q(x,y) \land \neg R(y,z)))
\end{aligned}$$

Problem 6: [6 pts] Prove or disprove the following statements:

(a) For all integers a, b, c, if $a|c$ and $b|c$, then $ab|c^2$.

(b) For all integers a, b, if $a|b$ and $b|a$, then $a = b$.

Answer: (a) True. If $c = ak$ and $c = bl$, then $c^2 = ab(kl)$, so $ab|c^2$.

(b) False. Set $a = 1$ and $b = -1$.

Grading Scheme: 3,3

Problem 7: [8 pts] Give an example of two uncountable sets A and B such that $A - B$ is

(a) finite.

(b) countably infinite.

(c) uncountable.

Answer: In each case, let us take A to be the set of real numbers.

(a) We can let B be the set of real numbers as well; then $A - B = \emptyset$, which is finite.

(b) We can let B be the set of real numbers that are not positive integers; in symbols, $B = A - \mathbf{Z}^+$. Then, $A - B = \mathbf{Z}^+$, which is countably infinite.

(c) We can let B be the set of positive real numbers. Then $A - B$ is the set of negative real numbers and 0, which is certainly uncountable.

Grading Scheme: 2,3,3

Student ID: ____________

Problem 8: [8 pts] Prove the following statement by contradiction.

"For any non-zero real number x, if $x + \frac{1}{x} < 2$, then $x < 0$".

Answer: Assume $x + \frac{1}{x} < 2$ and $x > 0$. We have

$$\begin{aligned}
& x + \frac{1}{x} < 2 \\
\rightarrow\ & \frac{x^2+1}{x} < 2 \\
\rightarrow\ & x^2 + 1 < 2x \qquad \text{since } x > 0 \\
\rightarrow\ & x^2 - 2x + 1 < 0 \\
\rightarrow\ & (x-1)^2 < 0
\end{aligned}$$

This contradicts with the fact that $(x-1)^2 \geq 0$, completing the proof.

Problem 9: [6 pts] Suppose that a and b are integers, $a \equiv 11 \pmod{19}$, and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \leq c \leq 18$ such that

(a) $c \equiv a - b \pmod{19}$

(b) $c \equiv 7a + 3b \pmod{19}$

(c) $c \equiv ab^2 \pmod{19}$

Answer: (a) 8

(b) 10

(c) 4

Grading Scheme: 2,2,2

Student ID: ____________

Problem 10: [12 pts] Solve each of these congruences with $0 \le x \le 103$ and $0 \le y \le 103$ using the result $15 \cdot 7 \equiv 1 \pmod{104}$.

(a) $7x \equiv 31 \pmod{104}$

(b) $15x + 41 \equiv 18 \pmod{104}$

(c) $49x \equiv 11 \pmod{104}$

(d)
$$\begin{cases} 9x + 2y \equiv 10 \pmod{104} \\ x + y \equiv 1 \pmod{104} \end{cases}$$

Answer: (a)

$$\begin{aligned} & 7x \equiv 31 \pmod{104} \\ \rightarrow\ & 15 \cdot 7x \equiv 15 \cdot 31 \pmod{104} \\ \rightarrow\ & x \equiv 49 \pmod{104} \end{aligned}$$

(b)

$$\begin{aligned} & 15x + 41 \equiv 18 \pmod{104} \\ \rightarrow\ & 15x \equiv -23 \pmod{104} \\ \rightarrow\ & 7 \cdot 15x \equiv 7(-23) \pmod{104} \\ \rightarrow\ & x \equiv 7(-23) \pmod{104} \\ \rightarrow\ & x \equiv 47 \pmod{104} \end{aligned}$$

(c)

$$\begin{aligned} & 49x \equiv 11 \pmod{104} \\ \rightarrow\ & 15 \cdot 7 \cdot 7x \equiv 15 \cdot 11 \pmod{104} \\ \rightarrow\ & 7x \equiv 61 \pmod{104} \\ \rightarrow\ & 15 \cdot 7x \equiv 15 \cdot 61 \pmod{104} \\ \rightarrow\ & x \equiv 83 \pmod{104} \end{aligned}$$

(d) We have $9x + 2y + (-2)(x + y) \equiv 10 - 2 \pmod{104}$, which is $7x \equiv 8 \pmod{104}$. So,

$$\begin{aligned} & 7x \equiv 8 \pmod{104} \\ \rightarrow\ & 15 \cdot 7x \equiv 15 \cdot 8 \pmod{104} \\ \rightarrow\ & x \equiv 16 \pmod{104} \end{aligned}$$

When $x = 16$, we have $16 + y \equiv 1 \pmod{104}$, and thus $y \equiv -15 \equiv 89 \pmod{104}$.

Grading Scheme: 2,3,3,4

Problem 11: [12 pts] Consider Bob is using RSA algorithm for public key cryptography. Bob starts by picking the two prime numbers $p = 43$ and $q = 23$. So, $n = pq = 989$.

(a) Bob's public key is a pair $(989, e)$. Which of the following integer(s) can Bob use for e? Why?

(i) 21; (ii) 7; (iii) 25; (iv) 11

(b) Suppose Bob chooses $e = 53$. What is the private key d? Show the steps of the extended Euclidean algorithm.

(c) Suppose Bob's public key is $(989, 53)$ and Alice wants to send a message $m = 720$ to Bob. Write down the modular expression that computes the encrypted message c. It is not necessary to evaluate the expression.

Answer: (a) (iii). We have $T = (p-1)(q-1) = 42 \cdot 22 = 924$. Bob can use 25 as this is the only choice such that $\gcd(25, 924) = 1$.

(b) The private key should satisfy $ed \equiv 1 (\text{mod } T)$, i.e., d is the multiplicative inverse of e in Z_T. Run the extended Euclidean algorithm to find d:

$$\begin{aligned}
924 &= 53 \cdot 17 + 23 \\
53 &= 23 \cdot 2 + 7 \\
23 &= 7 \cdot 3 + 2 \\
7 &= 2 \cdot 3 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

Then,

$$\begin{aligned}
1 &= 7 - 2 \cdot 3 \\
&= 7 - (23 - 7 \cdot 3) \cdot 3 \\
&= 7 \cdot 10 + 23 \cdot (-3) \\
&= (53 - 23 \cdot 2) \cdot 10 + 23 \cdot (-3) \\
&= 23 \cdot -23 + 53 \cdot (10) \\
&= (924 - 53 \cdot 17) \cdot -23 + 53 \cdot (10) \\
&= 53 \cdot 401 + 924 \cdot (-23)
\end{aligned}$$

Thus, $d = 401$.

(c) The encrypted message $c = 720^{53} \bmod 989$.

Grading Scheme: 3, 6, 3

Student ID: ____________

Problem 12: [8 pts] Evaluate the following expression by repeated squaring method. Show the steps.

$$8^{1027} \bmod 22$$

Answer: By the repeated squaring method, we have

$$\begin{aligned}
8^{2^0} &\equiv 8 \pmod{22}\\
8^{2^1} &\equiv 8^2 \equiv 20 \pmod{22}\\
8^{2^2} &\equiv 20^2 \equiv 4 \pmod{22}\\
8^{2^3} &\equiv 4^2 \equiv 16 \pmod{22}\\
8^{2^4} &\equiv 16^2 \equiv 14 \pmod{22}\\
8^{2^5} &\equiv 14^2 \equiv 20 \pmod{22}
\end{aligned}$$

We have $1027 = 2^0 + 2^1 + 2^{10}$.

$8^{2^{10}} \equiv 4 \pmod{22}$ since $8^{2^i} \equiv 4 \pmod{22}$ if $i \equiv 2 \pmod{4}$.

$$\begin{aligned}
8^{1027} &\equiv 8^{2^0+2^1+2^{10}} \pmod{22}\\
&\equiv 8^{2^0} \cdot 8^{2^1} \cdot 8^{2^{10}} \pmod{22}\\
&\equiv 8 \cdot 20 \cdot 4 \pmod{22}\\
&\equiv 2 \pmod{22}
\end{aligned}$$

Therefore, we have $8^{1027} \bmod 22 = 2$

Bonus Problem: [10 pts] An enemy tank is moving at a constant speed along a road. You can imagine the road as the infinite number line, where every position is identified by a number. The tank starts at time 0 at an unknown location x and moves at an unknown speed of y meters a minute, but we know that x and y are both positive integers. We can fire a cannon every minute at a specific location, but cannot see the tank. Can you design a strategy that guarantees to hit the tank eventually?

Answer: The Cartesian product $\mathbf{Z}^+ \times \mathbf{Z}^+$ is countable, and we can enumerate the pairs $(x, y) \in \mathbf{Z}^+ \times \mathbf{Z}^+$ one by one. At time i, we use the i-th pair (x, y) in this enumeration to decide the firing location. Note that if (x, y) are correct, the tank will be at position $x + y \cdot i$, so we fire at this location. Because every pair (x, y) will eventually be enumerated, we are guaranteed to hit the tank.