Discrete Structures for Computing

CS2214B, winter 2019

Midterm exam

March 11, 11:40 -13:20

100 points max

STUDENT NUMBER: _____

STUDENT NAME: _____

Problems	1	2	3	4	5	Total
Marks						

Guidelines

- There are 5 problems on Pages 1 and 2 followed by reference tables and formulas extracted from the course lectures on Page 3.
- Write down your name and student number on the booklet.
- Write your answers on the booklet.
- This is a closed-book exam and no electronic devices are allowed.
- You must return together both this exam statement and the booklet.

Problem 1 (20 points) Consider a universe U made of three things: fleegles, snurds and thingamabobs. Consider the following 3 predicates defined over U:

- $F(x)$: x is a fleegle,
- $S(x)$: x is a snurd,
- $T(x)$: x is a thingamabob.

Translate into predicate logic the following statements:

1. "Nothing is a snurd."
2. "All fleegles are snurds."
3. "Some fleegles are thingamabobs."
4. "No snurd is a thingamabob."
5. If any fleegle is a snurd then it is also a thingamabob."

Solution 1

1. $(\forall x)\ \neg S(x)$

2. $(\forall x)\ \ F(x) \ \rightarrow\ S(x)$
3. $(\exists x)\ \ (F(x) \wedge T(x))$
4. $(\forall x)\ \ (S(x) \ \rightarrow\ \neg T(x))$
5. $(\forall x)\ \ (F(x) \wedge S(x)) \ \rightarrow\ T(x)$

Problem 2 (20 points) Professor Cuthbert Calculus has designed a machine which consists of three components A, B, C which are either running or stopped. The constraints on those components are the following:

1. if A is running, then at least one of the components B or C is stopped,
2. if B is stopped, then at least one of the components A or C is running,
3. if C is running, then B is running as well.

Can the machine of Professor Cuthbert Calculus be built, that is, is the conjunction of the above three statements satisfiable. Justify your answer.

Solution 2 Let us denote by A, B, C Boolean variables stating that the respective components A, B, C are running. Then the 3 constraints can be rephrased as follows in propositional logic:

1. $A \ \ \rightarrow \ \ (\neg B \vee \neg C)$,
2. $\neg B \ \ \rightarrow \ \ (A \vee C)$,
3. $C \ \ \rightarrow \ \ B$.

Because of the third constraint, namely $C \ \rightarrow\ B$, it is natural to test whether the conjunction of the three constraints is satisfiable with $B = C = \mathsf{true}$. Then, since $\neg B \vee \neg C = \mathsf{false}$, to satisfy the first constraint, we must have $A = \mathsf{false}$. With those values of the Boolean variables A, B, C, the second constraint is satisfied. Therefore, the the machine of Professor Cuthbert Calculus be built.

Problem 3 (20 points)

1. Find all integers x such that $0 \leq x < 15$ and $2x + 14 \equiv 13 \mod 15$. Justify your answer.
2. Find all integers x such that $0 \leq x < 15$, $x \equiv 4 \mod 3$ and $x \equiv 6 \mod 5$. Justify your answer.
3. Find all integers x and y such that $0 \leq x < 15$, $0 \leq y < 15$, $x + y \equiv 12 \mod 15$ and $x - y \equiv 1 \mod 15$. Justify your answer.

Solution 3

1. We have $2 \times 7 \equiv 14 \equiv -1 \mod 15$. Hence, the equation

$$2x + 14 \equiv 13 \mod 15$$

is equivalent to

$$-x+ \equiv 7 \times (-14 + 13) \mod 15$$

leading to

$$x+ \equiv 7 \mod 15$$

2. We apply the Chinese Remainder Theorem (see the cheat sheet below). Hence, we have $m = 3$, $n = 5$, $a = 4$, $b = 6$. We need s and t such that $s\,m + t\,n = 1$, hence we can choose $s = 2$ and $t = -1$. Then, we have

$$c \equiv a + (b - a)\, s\, m \equiv 4 + (6 - 4) \times 2 \times 3 \equiv 1 \mod 15.$$

3. Adding the two equations side-by-side yields

$$2\,x+ \equiv 13 \mod 15.$$

Multiplying both side by 7

$$-x \equiv 91 \mod 15,$$

That is,

$$x \equiv -1 \equiv 14 \mod 15,$$

Problem 4 (20 points) Consider the affine cipher model $c = f(p))$ where the function f is defined by:

$$f : \begin{array}{ccc} \mathbb{Z}_{26} & \rightarrow & \mathbb{Z}_{26} \\ p & \longmapsto & 3\,p + 2 \ (\textbf{mod } 26) \end{array}$$

1. Prove that f is injective.
2. Prove that f is surjective.
3. Determine the inverse function f^{-1}.
4. Produce the ciphertext for "ABC"

Solution 4

1. Let us prove that f is injective. Let p_1 and p_2 in $\mathbb{Z}_{26}$ such that $f(p_1) = f(p_2)$ holds. We deduce $3p_1 + 2 \equiv 3p_2 + 2 \mod 26$. This yields

$$3(p_1 - p2) \equiv 0 \mod 26. \tag{1}$$

Since $\gcd(3, 26) = 1$ holds, let us find $3\,s + 26\,t = 1$ holds. We choose $s = 9$ and $t = -1$. Returning to Equation (1) we deduce:

$$9 \times 3(p_1 - p2) \equiv 9 \times 0 \mod 26,$$

that is,

$$(p_1 - p2) \equiv 0 \mod 26,$$

which implies $p_1 = p_2$ (since $p_1, p_2 \in \mathbb{Z}_{26}$), that is, f is injective.

2. Let us prove that f is surjective. For $c \in \mathbb{Z}_{26}$, let us search for the pre-images p of c by f, that is, let us solve $c = f(p)$. Since $3 \times 9 \equiv 1 \mod 26$ holds, we deduce:

$$\begin{array}{rcl} c = f(p) & \iff & c \equiv 3p_2 + 2 \mod 26, \\ & \iff & p \equiv 9(c-2) \mod 26. \end{array}$$

   Therefore, every $c \in \mathbb{Z}_{26}$ has a pre-image by f, namely $9(c-2)$.
3. From the previous calculation, we have

$$f^{-1} : \begin{array}{ccc} \mathbb{Z}_{26} & \to & \mathbb{Z}_{26} \\ c & \longmapsto & 9(c-2) \ (\textbf{mod } 26) \end{array}$$

4. We need to compute $f(0)$, $f(1)$ and $f(2)$ which are respectively 2, 5, 8. Therefore, the ciphertext for "ABC" is "CFI" .

Problem 5 (20 points) Prove by induction that for all $n \geq 1$ the integer $11^n - 1$ (that is, the n-th power of 11 minus 1) is divisible by 10.

Solution 5 Define the predicate $P(n)$ as $11^n - 1$ is multiple of 10. We shall prove that $P(n)$ is true for all $n \geq 1$, using *mathematical induction*.

Base case: For $n = 1$ we have $11^n - 1 = 10$ hence, the property $P(1)$ holds.

Inductive step: Let us assume for $P(k)$ holds for some $k \geq 1$ and let is prove that $P(k+1)$ holds as well. We have

$$11^{k+1} - 1 = 11 \times (11^k - 1) + 11 - 1 = 11 \times (11^k - 1) + 10.$$

From the induction hypothesis, there exists $q \in \mathbb{Z}$ such that $11^k - 1 = 10\,q$. Hence we have:

$$11^{k+1} - 1 = 11 \times 10\,q + 10 = 10\,(11q + 1).$$

Thus $P(k+1)$ holds as well.

Finally, from the theorem of mathematical induction, we have proved that $P(n)$ is true for all $n \geq 1$,

Reference tables and slides from the lectures

The Chinese Remainder Theorem Let m and n be two relatively prime integers. Let $s, t \in \mathbb{Z}$ be such that $s\,m + t\,n = 1$. The *Chinese Remaindering Theorem* states that for every $a, b \in \mathbb{Z}$ there exists $c \in \mathbb{Z}$ such that

$$(\forall x \in \mathbb{Z}) \quad \begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \iff x \equiv c \mod m\,n \tag{2}$$

where a convenient c is given by

$$c \;=\; a + (b-a)\,s\,m = b + (a-b)t\,n. \tag{3}$$

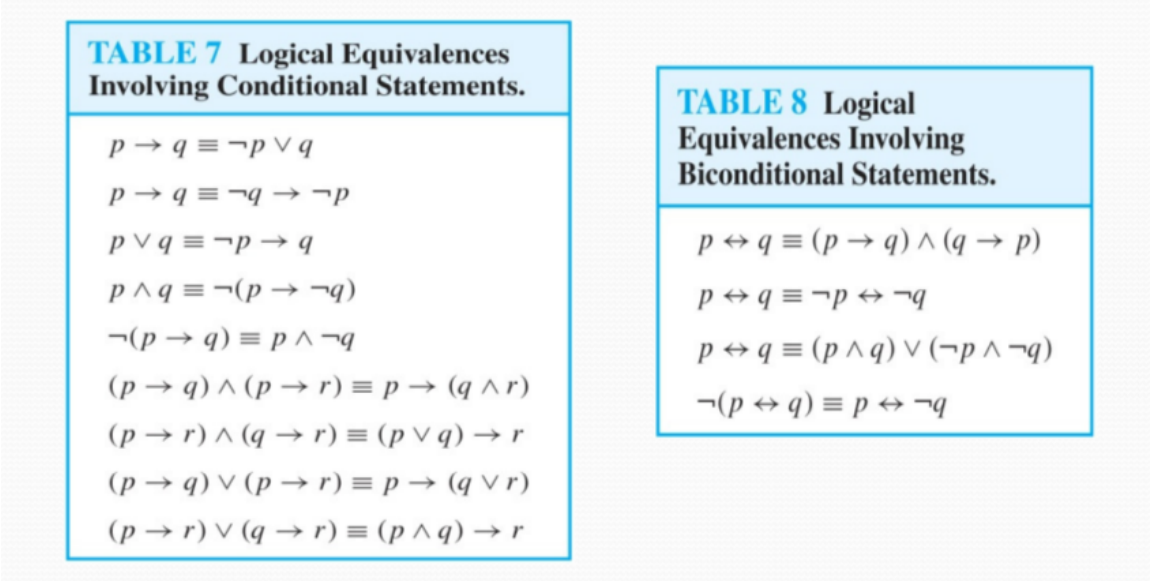

TABLE 7 Logical Equivalences Involving Conditional Statements.

$p \to q \equiv \neg p \vee q$

$p \to q \equiv \neg q \to \neg p$

$p \vee q \equiv \neg p \to q$

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

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

$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$

$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$

$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

TABLE 8 Logical Equivalences Involving Biconditional Statements.

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$