Midterm

Engineering 3422, 2005

Wednesday, October 19

Name: **Solution** Student Number: **3.41592**

Q0[8]. In this question all variables represent integers.

"True necessarily", "false necessarily", or "depends on the integers", in each case.

- If $a \mid b$ and $a \mid c$ then $ka \mid k(b+c)$. *true necessarily*
- If $m \mid (a+b)$ then $a \equiv b \pmod{m}$. *depends on the integers*
- If $a \equiv b \pmod{m}$ then $ka \equiv kb \pmod{m}$. *true necessarily*
- If $b \neq 0$ and $a = qb + r$ then $0 \leq r < |b|$. *depends on the integers*

Q1[6]. In this question, variables P and Q are boolean, while S, T, and V are sets. A and B are predicates on values in S.

Classify each of the following sentences as "tautology", "contradiction", "conditional sentence".

- $P \wedge (P \vee Q) \leftrightarrow P \wedge Q$ *conditional sentence*
- $(S - T) \cup (S - V) = S - (T \cup V)$ *conditional sentence*
- $(\forall x \in S, A(x)) \wedge (\forall x \in S, B(x)) \leftrightarrow (\forall x \in S, A(x) \wedge B(x))$ *tautology*

Q2[6] Let x and y be predicates on time, where time is represented by the natural numbers, $\mathbb{N}$.

Express the following statements about x and y using quantifier notation.

(a) Whenever x is true, y will be true at some later time.

$$(\forall t \in \mathbb{N}, x(t) \rightarrow (\exists u \in \mathbb{N}, u > t \wedge y(u)))$$

(b) x is be true infinitely often.

There are many ways to state this

$$(\exists t \in \mathbb{N}, x(t)) \wedge (\forall t \in \mathbb{N}, x(t) \rightarrow (\exists u \in \mathbb{N}, u > t \wedge x(u)))$$

Also acceptable would be

$$|\{t \in \mathbb{N} \mid x(t)\}| \notin \mathbb{N}$$

(c) y is be true exactly once.

$$(\exists t \in \mathbb{N}, y(t)) \wedge (\forall u \in \mathbb{N}, \forall v \in \mathbb{N}, u \neq v \rightarrow \neg y(v) \vee \neg y(u))$$

or

$$(\exists t \in \mathbb{N}, y(t) \wedge (\forall u \in \mathbb{N}, u \neq t \rightarrow \neg y(u)))$$

Also acceptable would be

$$|\{t \in \mathbb{N} \mid y(t)\}| = 1$$

Q3[10]. Give an algebraic proof that $(P \rightarrow Q) \vee (Q \rightarrow P)$ is a tautology.

To show that $(P \rightarrow Q) \vee (Q \rightarrow P)$ is a tautology, we must show that $(P \rightarrow Q) \vee (Q \rightarrow P) \Leftrightarrow T$.

$$\begin{array}{ll} & (P \rightarrow Q) \vee (Q \rightarrow P) \\ \Leftrightarrow & (\neg P \vee Q) \vee (\neg Q \vee P) \text{ Defintion of implication (twice)} \\ \Leftrightarrow & (\neg P \vee P) \vee (Q \vee \neg Q) \text{ Associativity and commutativity of } \vee \\ \Leftrightarrow & T \vee T \text{ Excluded middle} \\ \Leftrightarrow & T \text{ Domination} \end{array}$$

Note that it would aslo be acceptable to show that $T \Rightarrow (P \rightarrow Q) \vee (Q \rightarrow P)$. However, showing that $(P \rightarrow Q) \vee (Q \rightarrow P) \Rightarrow T$ is just pointless as we can infer T every propositional formula A, regardless of whether it is a tautology.

Q4[10]. From the definitions of divides ($|$) and congruence ($\equiv$), prove that for all integers a, b, c, and m, if $m \mid a$ and $m \mid b$ then $a + c \equiv b + c \pmod{m}$.

Proof.

Let $a, b, c,$ *and* m *be any integers at all, such that* $m \mid a$ *and* $m \mid b$.

Let q_0 *be an integer such that* $mq_0 = a$*; such an integer exists since* $m \mid a$*, by the definition of divides.*

Let q_1 *be an integer such that* $mq_1 = b$*; such an integer exists since* $m \mid b$*, by the definition of divides.*

Let $q = q_0 + q_1$.

$$\begin{aligned} & (a + c) - (b + c) \\ = \; & a - b \\ = \; & mq_0 + mq_1 \\ = \; & m(q_0 + q_1) \\ = \; & mq \end{aligned}$$

Since $(a + c) - (b + c) = mq$*, we have* $m \mid (a + c) - (b + c)$*, by the definition of divides.*

Since $m \mid (a + c) - (b + c)$*, we have* $a + c \equiv b + c \pmod{m}$*, by the definition of congruence.*