Midterm – Solution

Engineering 3422, 2004

Friday, October 22

Q0[6]. In this question all variables represent integers.

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

- If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ then $a \equiv b \pmod{mn}$ *Depends on the integers. This looks a lot like the Chinese Remainder Theorem, but the CRT requires that m and n be relatively prime. Consider $m = 4$, $n = 6$ and $a = 12$, $b = 24$.*

- If $m \mid a$ and $m \mid b$ then $m \mid ab$ *Necessarily true. $qm = ab$ where $q = q_0 q_1$ and $a = q_0 m$, $b = q_1 m$.*

- If $10 \mid a$ and $11 \mid a$ and $|a| < 100$. *Depends on the integers. Consider $a = 0$.*

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

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

- $P \wedge (P \to Q) \leftrightarrow P \wedge Q$ *Tautology*

- $S \cup (T - S) = S \cup T$ *Tautology*

- $P \wedge (Q \leftrightarrow \neg P) \wedge Q$ *Contradiction. Clearly P and Q must be T, but the middle conjunct says they are not equal.*

- $\exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x > y$ *Contradiction. This says that some integer is larger than all integers (even itself!).*

- $\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}, x > y$ *Tautology. This says that for every integer, there is a larger integer.*

- $(\exists x \in S, A(x)) \wedge (\exists x \in S, B(x)) \rightarrow (\exists x \in S, A(x) \wedge B(x))$ *Conditional sentence. Consider S being the integers and A being the property of being even and B being the property of being odd; the antecedent is true, while the consequent is false; so the implication is false. Now consider where A and B are the same property; the implication is true.*

Q2[4] Express using quantifier notation and the divisibility relation. S and T are sets of integers .

- Every integer in S divides some integer in T.

$$\forall a \in S, \exists b \in T, (a \mid b)$$

- No integer in S divides any integer in T.

$$\begin{aligned} \neg \exists a &\in S, \exists b \in T, (a \mid b) \\ \forall a &\in S, \forall b \in T, \neg\, (a \mid b) \\ \forall a &\in S, (\neg \exists b \in T, (a \mid b)) \end{aligned}$$

- A unique integer in S divides every integer in T.

$$(\exists a \in S, \forall b \in T, a \mid b) \wedge \forall a_0 \in S, \forall a_1 \in S, ((\forall b \in T, a_0 \mid b) \wedge (\forall b \in T, a_1 \mid b) \rightarrow a_0 = a_1)$$

$$(\exists a \in S, \forall b \in T, a \mid b) \wedge \neg \exists a_0 \in S, \exists a_1 \in S, (a_0 \neq a_1 \wedge (\forall b \in T, a_0 \mid b) \wedge (\forall b \in T, a_1 \mid b))$$

$$|\{a \in S \mid \forall b \in T, (a \mid b)\}| = 1$$

Q3[10]. Directly from the definitions of congruence and divisibility, show that, for all integers a and b, if $a \equiv 2 \pmod 5$ and $b \equiv 3 \pmod 5$ then $ab \equiv 1 \pmod 5$

- *Let a and b be any integers such that $a \equiv 2 \pmod 5$ and $b \equiv 3 \pmod 5$*

- *Since $a \equiv 2 \pmod 5$, by the definition of congruence, $5 \mid a - 2$.*

- *Since $b \equiv 3 \pmod 5$, by the definition of congruence, $5 \mid b - 3$.*

- *Since* $5 \mid a-2$, *by the definition of divisibility, there is an integer* q_0 *such that* $5q_0 = a-2$
- *Since* $5 \mid b-3$, *by,the definition of divisibility, there is an integer* q_1 *such that* $5q_1 = b-3$
- *So* $a = 5q_0+2$ *and* $b = 5q_1+3$.

$$\begin{aligned} ab &= (5q_0+2)(5q_1+3) \\ &= 25q_0q_1 + 15q_0 + 10q_1 + 6 \\ &= 5(5q_0q_1 + 3q_0 + 2q_1 + 1) + 1 \end{aligned}$$

- *Let* $q = (5q_0q_1 + 3q_0 + 2q_1 + 1)$. *So* $ab - 1 = 5q$.
- *By the definition of divisibility* $5 \mid ab-1$.
- *By the definition of congruence* $ab \equiv 1 \pmod 5$.

Q4[4]. Simplify as much as possible

- $\{x \in \mathbb{N} \mid \exists m \in \mathbb{N}, x = 7-2m\} = \{1,3,5,7\}$
- $(\forall a \in \mathbb{N}, \forall b \in \mathbb{N}, \exists x \in \mathbb{N}, \exists m \in \mathbb{N}, x = a - bm) \Leftrightarrow T$

  Since this is a sentence with no free variables, it must be T *or* F . *The Euclidean algorithm lemma says it is* T.

Q5[10]. Show that for all sets A and B, $A \cap B = A \cap \overline{B}$ implies that $A = \emptyset$.

Proof by contradiction.

- *Let* A *and* B *be any sets such that* $A \cap B = A \cap \overline{B}$.
- *Assume (falsely) that* $A \neq \emptyset$
- *Let* x *be any member of* A.
- *Either* $x \in B$ *or* $x \in \overline{B}$
- *Case* $x \in B$

- *Since $x \in A$ and $x \in B$, $x \in A \cap B$*
- *Since $A \cap B = A \cap \overline{B}$, $x \in A \cap \overline{B}$*
- *Thus $x \in \overline{B}$.*
- *This contradicts that $x \in B$.*

- *Case $x \in \overline{B}$*
  - *Since $x \in A$ and $x \in \overline{B}$, $x \in A \cap \overline{B}$*
  - *Since $A \cap B = A \cap \overline{B}$, $x \in A \cap B$*
  - *Thus $x \in B$.*
  - *This contradicts that $x \in \overline{B}$.*

Proof by calculation (not the easiest way, in this case)

- *Let A and B be any sets such that $A \cap B = A \cap \overline{B}$.*

$$
\begin{aligned}
& \emptyset \\
= \; & (A \cap B) \cap \overline{(A \cap B)} \text{ Complement law} \\
= \; & (A \cap B) \cap \overline{\left(A \cap \overline{B}\right)} \text{ Since } A \cap B = A \cap \overline{B} \\
= \; & (A \cap B) \cap \left(\overline{A} \cup B\right) \text{ De Morgan \& involution} \\
= \; & (A \cap \overline{A} \cap B) \cup (A \cap B) \text{ Distributivity \& idempotence} \\
= \; & \emptyset \cup (A \cap B) \text{ Complement and domination} \\
= \; & (A \cap B) \text{ Identity} \\
= \; & (A \cap B) \cup (A \cap B) \text{ Idempotence} \\
= \; & (A \cap B) \cup (A \cap \overline{B}) \text{ Since } A \cap B = A \cap \overline{B} \\
= \; & (A \cup A) \cap (A \cup B) \cap (A \cup \overline{B}) \cap (B \cup \overline{B}) \text{ Distributivity} \\
= \; & A \cap (A \cup B) \cap (A \cup \overline{B}) \text{ Idempotence, complement, \& identity} \\
= \; & A \text{ Absorption (twice)}
\end{aligned}
$$

The last step uses an absorption law, which says in general that

$$A \cap (A \cup C) = A.$$