University of Washington
Department of Computer Science and Engineering
CSE 311, Autumn 2011

# Quiz Section, October 20, 2011

Homework Review

1. Translate these statements into English, where R(x) is "x is a rabbit" and H(x) is "x hops" and the domain consists of all animals.

   (a) $\forall x(R(x) \wedge H(x))$

   Correct: "All animals are rabbits and hop," "All animals are hopping rabbits," "All animals are rabbits and all animals hop" (the last is not a direct translation, but a translation of the equivalent statement: $\forall x R(x) \wedge \forall x H(x)$, so it's OK)

   Common incorrect answer: "All rabbits hop." (Notice that this is a much weaker statement than saying that all animals are rabbits who hop.)

   (b) $\exists x(R(x) \rightarrow H(x))$

   Correct: "There is an animal that hops if it is a rabbit," "There is an animal such that if it is a rabbit, then it hops," "There is an animal that hops or is not a rabbit" (The last is a translation of the equivalent statement (by law of implication): $\exists x(H(x) \vee \neg R(x))$)

   Common incorrect answers: "There is a rabbit that hops," "There is an animal that hops because it is a rabbit" (Notice that these are incorrect because they assert the existence of a rabbit, while the statement itself is true even if no rabbits exist.)

2. Determine whether $\forall x(P(x) \leftrightarrow Q(x))$ and $\forall x P(x) \leftrightarrow \forall x Q(x)$ are logically equivalent.

   These statements are not equivalent.

   In order to be equivalent, the left side and right side must have the same truth value no matter what domain we use and no matter what predicates we substitute for P(x) and Q(x).

   So in the following proof we will show that for some specific predicates and some specific members of the domain, the statements do not have the same truth value and thus are not equivalent.

*Proof.*

Let the domain be all integers. Let $P(x) =$ "x is odd". Let $Q(x) =$ "x is even",
Let $c = 1$, Let $d = 2$.

| | | |
|---|---|---|
| $P(c)$ | definition of P(x) | (1) |
| $\neg Q(c)$ | definition of Q(x) | (2) |
| $\neg P(d)$ | definition of P(x) | (3) |
| $\neg(P(c) \leftrightarrow Q(c))$ | 1, 2, definition of "if and only if" | (4) |
| $\exists x \neg(P(x) \leftrightarrow Q(x))$ | 4, existential generalization | (5) |
| $\neg\forall x(P(x) \leftrightarrow Q(x))$ | 5, rules for negating quantifiers | (6) |
| $\exists x \neg P(x)$ | 3, existential generalization | (7) |
| $\neg\forall x P(x)$ | 7, rules for negating quantifiers | (8) |
| $\exists x \neg Q(x)$ | 2, existential generalization | (9) |
| $\neg\forall x Q(x)$ | 9, rules for negating quantifiers | (10) |
| $\forall x P(x) \leftrightarrow \forall x Q(x)$ | 8, 10, definition of "if and only if" | (11) |
| $\forall x(P(x) \leftrightarrow Q(x)) \not\equiv \forall x P(x) \leftrightarrow \forall x Q(x)$ | 6, 11, definition of equivalence | (12) |

$\square$

3. Show that the premises $(p \wedge t) \to (r \vee s)$, $q \to (u \wedge t)$, $u \to p$, and $\neg s$ imply the conclusion that $q \to r$ using the inference rules and equivalences. How many rows would you need if you tried to do this using a truth table?

   Note that one cannot apply inference rules to part of a statement. For example, it is not allowed to go directly from $q \to (u \wedge t)$ to $q \to u$ by simplification. Instead, you would have to take the following steps:

| | | |
|---|---|---|
| $q \to (u \wedge t)$ | Given | (1) |
| $(u \wedge t) \vee \neg q$ | Law of implication on 1 | (2) |
| $(u \vee \neg q) \wedge (t \vee \neg q)$ | Distribution on 2 | (3) |
| $(u \vee \neg q)$ | Simplification (eliminating AND) on 3 | (4) |
| $q \to u$ | Law of implication on 4 | (5) |

Here is a nice, short proof that utilizes the direct proof method. (It is also possible to prove this without using the direct proof method by applying a series of inferences and equivalences to the given premises.)

*Proof.*

| | | | |
|---|---|---|---|
| $(p \wedge t) \rightarrow (r \vee s)$ | | Given | (1) |
| $q \rightarrow (u \wedge t)$ | | Given | (2) |
| $u \rightarrow p$ | | Given | (3) |
| $\neg s$ | | Given | (4) |
| | $q$ | Assumption | (5) |
| | $u \wedge t$ | M.P. on 2, 5 | (6) |
| | $u$ | simplification (eliminating AND) on 6 | (7) |
| | $t$ | simplification on 6 | (8) |
| | $p$ | M.P. on 3, 7 | (9) |
| | $(p \wedge t)$ | conjunction (introducing AND) on 8, 9 | (10) |
| | $(r \vee s)$ | M.P. on 1, 10 | (11) |
| | $r$ | disj. syllogism (eliminating OR) on 4, 11 | (12) |
| $q \rightarrow r$ | | Direct Proof Rule | (13) |

□

4. Use rules of inference to show that if $\forall x(P(x) \vee Q(x))$ and $\forall x((\neg P(x) \wedge Q(x)) \rightarrow R(x))$ are true then $\forall x(\neg R(x) \rightarrow P(x))$ is also true, where the domains of all quantifiers are the same.

*Proof.*

| | | |
|---|---|---|
| $\forall x((\neg P(x) \wedge Q(x)) \rightarrow R(x))$ | given | (1) |
| $(\neg P(a) \wedge Q(a)) \rightarrow R(a)$ (for any $a$ in the domain) | universal instantiation on 1 | (2) |
| $\neg R(a) \vee \neg(\neg P(a) \wedge Q(a))$ | law of implication on 2 | (3) |
| $\neg R(a) \vee (P(a) \vee \neg Q(a))$ | De Morgan's on 3 | (4) |
| $(\neg R(a) \vee (P(a)) \vee \neg Q(a)$ | associativity on 4 | (5) |
| $\forall x(P(x) \vee Q(x))$ | given | (6) |
| $P(a) \vee Q(a)$ | universal instantiation on 6 | (7) |
| $(\neg R(a) \vee (P(a)) \vee P(a)$ | resolution on 5, 7 | (8) |
| $\neg R(a) \vee ((P(a) \vee P(a))$ | associativity on 8 | (9) |
| $\neg R(a) \vee P(a)$ | idempotent on 9 | (10) |
| $R(a) \rightarrow P(a)$ | law of implication on 10 | (11) |
| $\forall x(R(x) \rightarrow P(x))$ | universal generalization on 11 | (12) |

□

5. Prove or disprove: $n^2 + 3n + 1$ is always prime for integer $n > 0$.

   We disprove by counterexample:

   Let $n = 6$

   Then $n^2 + 3n + 1 = 55$, which is divisible by 5 and 11 and thus not prime.

New Stuff

1. Power Sets
   - $\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
   - $\mathcal{P}(\emptyset) = \{\emptyset\}$
   - $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$
   - How many elements in the power set of a set with $n$ elements? $2^n$

2. Cartesian Products

   $A = \{a, b, c\}$, $B = \{1, 2\}$
   - $A \times B = \{(a, 1), (a, 2), (b, 2), (b, 2), (c, 1), (c, 2)\}$
   - $B^2 = B \times B = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$
   - How many elements in the Cartesian Product of a set with $m$ elements and a set with $n$ elements? $mn$

3. Proofs with sets

   (a) Show that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$
   (7th: 2.1, #17; 6th: 2.1, #15)

   (b) Prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ if and only if $A \subseteq B$
   (7th: 2.1, #25; not in 6th ?)

   Note that to prove an "if and only if" statement, we need to show that the left side implies the right side AND that the right side implies the left side.

   Also note that to show that one set is a subset of another set, we need to show that any member of the first set is also a member of the second set.

*Proof.*
First we show that $\mathcal{P}(A) \subseteq \mathcal{P}(B) \to A \subseteq B$

| | | |
|---|---|---|
| Let $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ | assumption | (1) |
| Let $x \in A$ | assumption | (2) |
| $\{x\} \subseteq A$ | 2, definition of subset | (3) |
| $\{x\} \in \mathcal{P}(A)$ | 3, definition of power set | (4) |
| $\{x\} \in \mathcal{P}(B)$ | 1,4, definition of subset | (5) |
| $\{x\} \subseteq B$ | 5, definition of power set | (6) |
| $x \in B$ | 6, definition of subset | (7) |
| $(x \in A) \to (x \in B)$ | 2-7, direct proof rule | (8) |
| $A \subseteq B$ | 8, definition of subset | (9) |

$\mathcal{P}(A) \subseteq \mathcal{P}(B) \to A \subseteq B$ 1-9, direct proof rule

Next we show that $A \subseteq B \to \mathcal{P}(A) \subseteq \mathcal{P}(B)$

| | | |
|---|---|---|
| Let $A \subseteq B$ | assumption | (1) |
| Let $C \in \mathcal{P}(A)$ | assumption | (2) |
| $C \subseteq A$ | 2, definition of power set | (3) |
| $C \subseteq B$ | 1,3, and proof 3a (above) | (4) |
| $C \in \mathcal{P}(B)$ | 4, definition of power set | (5) |
| $(C \in \mathcal{P}(A)) \to (C \in \mathcal{P}(B))$ | 2-5, direct proof rule | (6) |
| $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ | definition of subset | (7) |

$A \subseteq B \to \mathcal{P}(A) \subseteq \mathcal{P}(B)$ 1-7, direct proof rule

We have shown that the left side implies the right side and that the right side implies the left side. Thus we have proven that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ if and only if $A \subseteq B$.

□

(c) Show that $\emptyset \times A = A \times \emptyset = \emptyset$
(7th: 2.1, #31; 6th: 2.1, #27)

(d) Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$
(7th: 2.2, #15; 6th: 2.2, #15)

i. With a membership table
ii. By showing that each set is a subset of the other
iii. By using set builder notation and logical equivalences

(e) Show that $A - B = A \cap \overline{B}$
(7th: 2.2, #19a)

(f) Show that $(A \cap B) \cup (A \cap \overline{B}) = A$
(7th: 2.2, #19b; 6th: 2.2, #19)

4. Mod arithmetic

   (a) What time does a 12-hour clock read:
   (7th: 4.1, #11; not in 6th?)

   - 80 hours after it reads 11:00 = 91 **mod** 12 = 7:00
   - 40 hours before it reads 12:00 = -28 **mod** 12 = 8:00
   - 100 hours after it reads 6:00 = 106 **mod** 12 = 10:00

   (b) Let $m$ be a positive integer. Show that $a \equiv b \pmod{m}$ if $a \textbf{ mod } m = b \textbf{ mod } m$
   (7th: 4.1, #15; 6th: 3.4, #11)

5. Functions

   (7th: 2.3, #21 6th: 2.3, #17)
   Give an explicit formula for a function from the set of integers to the set of positive integers that is

   (a) one-to-one but not onto.
   (b) onto but not one-to-one.
   (c) both onto and one-to-one.
   (d) neither one-to-one nor onto.