Exam 1 - Solutions

Inference Rules

1. For each candidate inference rule below, indicate if it is *sound* or *unsound* (circle the correct answer). For the rules that are unsound, provide a counterexample to show it is unsound. You do not need to provide any justification for the rules that are sound.

a. $\dfrac{P}{Q}$

Unsound. Choosing $Q = F$ and $P = T$ leads to a false conclusion, so the rule is unsound.

b. $\dfrac{P \wedge (P \implies Q)}{Q}$

Sound. To conclude Q, must have both P and $P \implies Q$.

c. $\dfrac{P \wedge Q}{P \vee Q}$

Sound. $P \wedge Q$ is True only when P and Q are both True, which guarantees $P \vee Q$.

d. $\dfrac{\overline{Q} \implies \overline{P}}{P \implies Q}$

Sound. This is the contrapositive inference rule (can verify with truth table).

e. $\dfrac{P \wedge \overline{P}}{P \implies \overline{P}}$

Sound. Since there is no way to make the antecedent True, the rule is sound regardless of the conclusion (it is just never useful).

Satisfiability

2. For each formula below, determine if it is *satisfiable* and if it is *valid*.

a. $(P \vee \overline{P})$

Satisfiable and *Valid*. Whatever we assign to P, either P or $\overline{P}$ must be true, so $P \vee \overline{P}$ is valid.

b. $(P \lor Q) \land (\overline{P} \lor Q)$

Satisfiable but *Not Valid*. Selecting $P = F$ and $Q = T$ shows that it is satisfiable; selecting $P = F$ and $Q = F$ shows that it is not valid since the first clause is not True.

c. $(P \implies Q) \lor (Q \implies P)$

Satisfiable and *Valid*. $P \implies Q$ is True for all inputs except $P = T, Q = F$. For that input, $Q \implies P$ is True.

Logical Formula

3. Show convincingly that P IMPLIES Q is logically equivalent to $\overline{P} \lor Q$.

We can show logical equivalence for small formulas by showing the truth table, to verify that the value of the formula is the same for all inputs:

P	Q	P $\implies Q$	$\overline{P} \lor Q$
T	**T**	**T**	**T**
T	**F**	**F**	**F**
F	**T**	**T**	**T**
F	**F**	**T**	**T**

Well Ordered Sets

4. Explain why the set of the integers ($\mathbb{Z}$) is not well ordered by $<$. (Expected answers will give a good intuitive reason; better-than-expected answers will provide a convincing proof.)

Intuitively, $\mathbb{Z}$ is not well-ordered by $<$ since the negative numbers extend to negative infinity so there is no smallest integer.

For a convincing proof, we use proof-by-contradiction.

For $\mathbb{Z}$ to be well ordered, every subset of $\mathbb{Z}$ must contain a minimum element. $\mathbb{Z} \subseteq \mathbb{Z}$, so if we can show $\mathbb{Z}$ has no minimum element, this show that $\mathbb{Z}$ is not well ordered.

Assume there is some minimum element $m \in \mathbb{Z}$.

The value, $m - 1$ is an integer since the integers are closed under subtraction. But $m - 1 < m$, so we have a contradiction: m is not the minimum element of $\mathbb{Z}$.

Thus, there is no minimum element in $\mathbb{Z}$. Since $\mathbb{Z}$ is a subset of $\mathbb{Z}$, this means $\mathbb{Z}$ is not well-ordered by $<$.

Relations

5. R is a total ([$\geq$ 1 arrow out]), injective ([$\leq$ 1 arrow in]), relation between A and B with graph $G \subseteq (A \times B)$. For each statement below, indicate if it *must be true*, *might be true* (could be either true or false), or *cannot be true* (must be false). Provide a short justification supporting your answer.

   a. $|A| \leq |B|$

   Must be True. Since R is total and injective, there must be at least one arrow out of each A element, and no more than one arrow into each B element. Thus, each A element has an arrow to a different B element, so there must be at least as many elements in B as there are in A (could be more in B since injective means $\leq$ 1 arrow in).

   b. $A = \emptyset \implies B = \emptyset$

   Cannot be True. This was a tricky question, since the "Might be True" option doesn't really make sense for an implication: if there is any way for $A = \emptyset$ to be true and $B = \emptyset$ to be false, then the implication is false. This is the case here when A is empty, B could have elements with no incoming arrows. (Because of the trickiness of the question, students received nearly full credit for the "Might Be True" answer with a good explanation.)

   c. $B = \emptyset \implies A = \emptyset$

   Must be True. If B is empty, A must also be empty since any arrows out of elements in A need to point to elements in B.

   d. R^{-1} (the inverse relation of R) is a surjective function.

   Must be True. Since R is injective, R^{-1} must be a function (flipping the arrows turns [$\leq$ 1 in] into [$\leq$ 1 out]). Since R is total, R^{-1} must be surjective (flipping the arrows turns [$\geq$ 1 out] into [$\geq$ 1 in]).

Proofs

6. Define the sets *People* and *UVA* as:

   $People$ ::= all people in the universe
   UVA ::= set of all students at UVA

   Assume these two axioms:

   1. $\forall s \in UVA.\ Honorable(s)$
   2. $\forall p \in People.\ Honorable(p) \implies \neg(Cheats(p) \lor Lies(p) \lor Steals(p))$

   Prove that if $p \in People$ and $Cheats(p)$, then p must not be a UVA student.

   Answer: The proposition to prove is $p \in People \land Cheats(p) \implies p \notin UVA$.

From axiom 2, $\forall p \in People.\, Honorable(p) \implies \neg(Cheats(p) \lor Lies(p) \lor Steals(p))$. Using De Morgan's law, this can be rewritten as, $Honorable(p) \implies (\neg Cheats(p)) \land (\neg Lies(p)) \land (\neg Steals(p))$. Since the conjuction is only true when all of its clauses are true, $Honorable(p) \implies \neg Cheats(p)$.

From axiom 1, $\forall s \in UVA.\, Honorable(s)$. Since we showed, $Honorable(p) \implies \neg Cheats(p)$, this means $\forall s \in UVA.\, \neg Cheats(s)$. Since any $\forall x \in Universe.\, x \in UVA \lor x \notin UVA$, we can conclude, $\forall p \in People.\, \neg Cheats(p) \implies p \notin UVA$.

Note that is it not necessary to argue that all UVA students are People for the proof to be valid! Since we have shown that $Cheats(x) \implies x \notin UVA$, we can draw x from any set we want and the implication is still true.

7. Below is a bogus proof that claims to prove every integer greater than 6 can be written as $3a + 5b$ for natural numbers a and b ($a, b \in \mathbb{N}$). Identify the first incorrect inference step, and explain clearly why it is wrong.

    a. We state the proposition as,

    $$P(n) ::= \exists a, b \in \mathbb{N}.\, n = 3a + 5b$$

    and prove $\forall n \in \mathbb{N}, n \geq 6.\, P(n)$.

    b. We prove using the well-ordering principle.

    c. Define the set of counter-examples, C:

    $$C ::= \{n \in \mathbb{N}, n \geq 6 | \forall a, b \in \mathbb{N}.\, n \neq 3a + 5b\}$$

    d. Assume C is non-empty.

    e. By well-ordering principle, there must be some minimum element of C, $m \in C$.

    f. We reach a contradiction by showing $P(m)$.

    g. Since m is the minimum element of C, we know $\forall k \in \mathbb{N}, 6 \leq k < m.\, P(k)$.

    h. We know $m > 6$ since $n \geq 6$ and $P(6)$ is true: $6 = 3 \cdot 2 + 5 \cdot 0$.

    i. Since $m - 3 < m$, this implies $P(m - 3)$.

    j. $P(m - 3)$ implies $\exists a, b \in \mathbb{N}.\, m - 3 = 3a + 5b$.

    k. So, $m = 3a + 5b + 3 = 3(a + 1) + 5b = 3a' + 5b$ for some $a' \in \mathbb{N}$.

    l. This shows $P(m)$, which is a contradiction since we selected $m \in C$. Hence, C must be empty, proving that $P(n)$ holds for all $n \in \mathbb{N}, n \geq 6$.

    Incorrect step: *i*.

    The problem is we cannot conclude $P(m - 3)$ since the set of counter-examples was limited to $n \geq 6$. Hence, we can only know that $P(m - 3)$ is not a counter-example (that is, it should have been a member of C) if $m - 3 \geq 6$. For this to be valid, we would need to show $m > 8$ by establishing $P(6)$, $P(7)$, and $P(8)$ (but, this is not possible since $P(7)$ is not true).

8. Prove by induction that every finite non-empty subset of the integers contains a *greatest* element, where an element $x \in S$ is defined as the greatest element if $\forall z \in S - \{x\}.\, x > z$.

    This problem is very similar to Problem 5 from Problem Set 5 (you just need to switch the comparison function and replace rationals with integers).

