Solutions To HW3

Zixuan Chen
X313572
zixuanchen@ucsb.edu

July 2024

Solution To Question 1

Theorem: If n and m are odd integers, then $n \cdot m$ is odd.

(a) Proof

Let n and m be odd integers. Then $n = 2k + 1$ and $m = 2j + 1$. Plugging into the expression $n \cdot m$ gives

$$n \cdot m = (2k + 1)(2j + 1) = 2(j \cdot k + j + k) + 1.$$

Since k and j are integers, $j \cdot k + j + k$ is also an integer. Then $n \cdot m$ equals two times an integer plus one, therefore $n \cdot m$ is odd.

Analysis:

The purple sentence is not complete. It should be: Since n is an odd integer, then $n = 2k + 1$ for some integer k. Since m is an odd integer, then $m = 2j + 1$ for some integer j. Moreover, the red formulas are not correct. They should be: $n \cdot m = (2k + 1)(2j + 1) = 2(2j \cdot k + j + k) + 1.$ and $2j \cdot k + j + k$

(b) Proof

Let n and m be odd integers. Since n is an odd integer, then $n = 2k + 1$ for some integer k. Since m is an odd integer, then $m = 2j + 1$ for some integer j. Plugging $2k + 1$ for n and $2j + 1$ for m into the expression $n \cdot m$ gives

$$n \cdot m = (2k + 1)(2j + 1).$$

Since $n \cdot m$ is equal to two times an integer plus one, then $n \cdot m$ is an odd integer.

Analysis:

This proof is missing the critical step of expanding the red formula and showing how it simplifies to $2 \times (\text{integer}) + 1$. Essential intermediate steps are skipped. It should be: $n \cdot m = (2k + 1)(2j + 1) = 2(2j \cdot k + j + k) + 1.$ Since k and j are integers, $2j \cdot k + j + k$ is also an integer. Then $n \cdot m$ equals two times an integer plus one

(c) Proof

Let n and m be odd integers. Since n is an odd integer, then $n = 2k + 1$ for some integer k. Since m is an odd integer, then $m = 2k + 1$ for some integer k. Plugging into the expression $n \cdot m$ gives

$$n \cdot m = (2k + 1)(2k + 1) = 2(2k^2 + 2k) + 1.$$

Since k is an integer, $2k^2 + 2k + 1$ is also an integer. Since $n \cdot m$ is equal to two times an integer plus one, then $n \cdot m$ is an odd integer.

Analysis:

This proof incorrectly assumes that m can be represented by the same variable as n.(the red part) This is incorrect because n and m are independent odd integers and should be expressed with different variables. Also, the purple part (if we accept the former error, it should be: $2k^2 + 2k$) will not make any sense even if we replace one k with another variable.

Solution To Question 2

Theorem: For all non-zero integers, x, y, z, if x does not divide yz, then x does not divide y.

(a) Proof and Analysis

We prove this by contrapositive. Let x, y, z be non-zero integers. We assume that x does divide y. Then $y = kx$(Skipped essential application of definition. Should be: Since x divides y, then there is an integer k, s.t. $y = kx$). So,

$$zy = z(kx) = (kz)x$$

Since z, k are integers, kz is also an integer. So, x divides zy.

(b) Proof and Analysis

We prove this by contrapositive. Let x, y, z be non-zero integers. We assume that x does divide y. So, $y = kx$ for some integer k. (Skipped Essential Steps Here: Multiply both side by z, we have $zy = z(kx) = (zk)x$. Since z, k are integers, thus zk is an integer as well.) Since zk is also an integer, we conclude that x divides zy, thus proving the theorem.

(c) Proof and Analysis

We prove this by contrapositive. Let x, y, z be non-zero integers. Assume that x divides y. So, $x = ky$ (Error: should be $y = kx$) for some integer k. Therefore, x divides yz if and only if $ky = ayz$ (Error: $akx = yz$ and we have $a = z$ as a witness) for some integer a. ~~We divide this out to get $a = \frac{k}{z}$.~~(Error: I don't get the point of writing this because it does not make any sense. Maybe this is a witness but, since the former step is wrong, it will not make sense.) Since k, z are both integers, kz is also an integer, thus proving that x divides yz.

Solution To Question 3

Statement: The sum of any two integers is odd if and only if at least one of them is odd.

(a) Define predicates and write the symbolic form

Let:

- $Q(x)$: x is odd.

$$\forall x \in \mathbb{Z} \forall y \in \mathbb{Z}(Q(x+y) \leftrightarrow (Q(x) \vee Q(y)))$$

(b) Disprove the statement

We can use a couterexample to disprove the statement: Let $x = 3$ and $y = 5$, then both $Q(x)$ and $Q(y)$ are **True**, thus $Q(x) \vee Q(y)$ is **True**. However, $x + y = 3 + 5 = 8$, which is an even number, thus $Q(x + y)$ is **False**.

$\therefore$ We **disprove** $\forall x \in \mathbb{Z} \forall y \in \mathbb{Z}(Q(x+y) \leftrightarrow (Q(x) \vee Q(y)))$.

Solution To Question 4

Statement: If x and y are integers such that $x + y \geq 5$, then $x > 2$ or $y > 2$.

(a)Symbolic Form with quantifiers

$$\forall x \in \mathbb{Z} \forall y \in \mathbb{Z}((x + y \geq 5) \to (x > 2) \vee (y > 2))$$

(b) Proof by contrapositive

Let x and y be integers. We assume that it is not true than x is less than 2 or y is less than 2 and we want to prove that $x + y$ is less than 5. Using De Morgan's Law, we have the assumption equivalent to $x \leq 2$ and $y \leq 2$. Adding the inequalities gives $x + y \leq 4$. Thus $x + y < 5$.

$\therefore$ The statement is proved.

Solution To Question 5

Statement: The average of two odd integers is an integer.

(a)Symbolic Form with quantifiers

Let:

- $Q(x)$: x is odd.

$$\forall x \in \mathbb{Z} \forall y \in \mathbb{Z}(Q(x) \wedge Q(y) \to \frac{x+y}{2} \in \mathbb{Z})$$

Direct Proof

Let x and y be integers. Since x, y are odd, $x = 2m + 1$ for some integer m and $y = 2n + 1$ for some integer n. Plugging in these 2 equations into $\frac{x+y}{2}$ gives

$$\frac{x+y}{2} = \frac{2m+1+2n+1}{2} = \frac{2(m+n+1)}{2} = m + n + 1$$

Since m and n are integers, $m + n + 1$ is an integer as well.

$\therefore \frac{x+y}{2}$ is an integer.

Solution To Question 6

Statement: For any three consecutive integers, their product is divisible by 6.

(a) Symbolic Form using quantifiers

Let:

- $D(a, b)$: a divides b.
- $S(x)$: $x \cdot (x + 1) \cdot (x + 2)$.

$$\forall x \in \mathbb{Z} \quad D(6, S(x))$$

(b) Direct Proof

Proof:

Assume x is an integer. Consider three consecutive integers x, $x + 1$, and $x + 2$.

To prove that $x(x + 1)(x + 2)$ is divisible by 6, we need to show it is divisible by both 2 and 3.

Divisibility by 2:

Let x be an integer. Whenever a number is divided 2 we will get the remainder is 0 or 1. Therefore, $x = 2q$ or $x = 2q + 1$ for some integer q. If $x = 2q$, then x and $x + 2 = 2q + 2 = 2(q + 1)$ are divisible by 2. If $x = 2q + 1$, then $x + 1 = 2q + 2 = 2(q + 1)$ is divisible by 2. Thus $x(x + 1)(x + 2)$ is divisible by 2.

Divisibility by 3:

Similarly, let x be an integer. Whenever a number is divided by 3 the remainder obtained is either 0 or 1 or 2. Therefore, $x = 3m$ or $x = 3m + 1$ or $x = 3m + 2$ for some integer m. If $x = 3m$, then x is divisible by 3. If $x = 3m + 1$, then $x + 2 = 3m + 3 = 3(m + 1)$ is divisible by 3. If $x = 3m + 2$, then $x + 1 = 3m + 3 = 3(m + 1)$ is divisible by 3. Therefore, $x(x + 1)(x + 2)$ is divisible by 3.

Divisibility by 6:

Since $x(x + 1)(x + 2)$ is divisible by both 2 and 3, thus it is divisible by the least common multiple of 2 and 3. Since 2 is not a factor of 3, their least common multiple is $2 \times 3 = 6$. Therefore, it's divisible by 6.

$$\therefore \forall x \in \mathbb{Z} \quad D(6, S(x))$$

Solution To Question 7

Basis Step: The string `()` is in S.

Recursive Steps:

- (a) If $x \in S$, then $(x) \in S$.
- (b) If $x \in S$ and $y \in S$, then $xy \in S$, where xy means the concatenation of x and y.

Prove: For any string $x \in S$, the number of left parentheses in x is equal to the number of right parentheses in x.

Let $L[x]$ return the number of left parentheses in x.
Let $R[x]$ return the number of right parentheses in x.

Theorem: $\forall s \in S \ (L[s] = R[s])$

Proof by Induction:

Base Case: $s = ()$. $L[()] = R[()] = 1$.

Inductive Step: Assuming that $x \in S$ and $y \in S$, then $L[x] = R[x]$ and $L[y] = R[y]$. Then we consider the following two cases depending on which was the last recursive rule.

Case 1: $s = (x)$, where $x \in S$.

We assume that $L[x] = R[x]$ and prove that $L[s] = R[s]$.

$$\begin{aligned} L[s] &= L[(x)] \quad \text{(Since } s = (x)\text{)} \\ &= 1 + L[x] \quad \text{(Since } (x) \text{ has one more (than } x\text{)} \\ &= 1 + R[x] \quad \text{(By the inductive hypothesis)} \\ &= R[(x)] \quad \text{(Since } (x) \text{ has one more) than } x\text{)} \\ &= R[s] \quad \text{(Since } s = (x)\text{)} \end{aligned}$$

Case 2: $s = xy$, where $x \in S$ and $y \in S$.

We assume the inductive hypothesis and prove that $L[s] = R[s]$.

$$\begin{aligned} L[s] &= L[xy] \quad \text{(Since } s = xy\text{)} \\ &= L[x] + L[y] \\ &= R[x] + R[y] \quad \text{(By the inductive hypothesis)} \\ &= R[xy] \\ &= R[s] \quad \text{(Since } s = xy\text{)} \end{aligned}$$

Therefore, $L[s] = R[s]$.

Solution To Question 8

(a) Calculate $removeTail(append((2,(3,[])),1))$

$$
\begin{aligned}
&removeTail(append((2,(3,[])),1)) \\
=&removeTail((2, append((3,[]),1))) \quad \text{(By Recursive Step of } append : n = 2, l = (3,[]), m = 1) \\
=&removeTail((2,3, append(([]),1))) \quad \text{(By Recursive Step of } append : n = 3, l = ([]), m = 1) \\
=&removeTail((2,3,1,[])) \quad \text{(By Basis Step of } append, m = 1) \\
=&removeTail((2, removeTail((3,1,[])))) \quad \text{(By Recursive Step of } removeTail : m = (2,3,1,[])) \\
=&(2,3, removeTail((1,[]))) \quad \text{(By Recursive Step of } removeTail : m = (3,1,[])) \\
=&(2,(3,[])) \quad \text{(By Basis Step of } removeTail : m = [])
\end{aligned}
$$

(b) Calculate $prepend(remove((1,(2,(2,(3,[])))),2),3)$

$$
\begin{aligned}
&prepend(remove((1,(2,(2,(3,[])))),2),3) \quad \text{(Base statement)} \\
=&prepend((1, remove((2,(2,(3,[]))),2)),3) \quad \text{(By recursive step of remove, } m = (2,(2,(3,[])))) \\
=&prepend((1,(2,(3,[]))),3) \quad \text{(By base step of remove, } m = (2,(3,[]))) \\
=&(3,(1,(2,(3,[])))) \quad \text{(By base step of prepend, } m = (3,(1,(2,(3,[])))))
\end{aligned}
$$

Solution To Question 9

(a) Demonstrate that this attempted proof is invalid by providing and justifying a counterexample (disproving the statement)

Solutions: Proof by counterexample.

Take $x = 1$ and $l' = (2,[])$ so that append(removeTail($(1,(2,[]))$), 1) = $(1,(2,[]))$.

Applying definitions, we have:

$$\text{LHS} = \text{append}((1,[]),1) = (1,(1,[])) \neq (1,(2,[])) = \text{RHS}$$

$$LHS \neq RHS$$

(b) Explain why the attempted proof is invalid by identifying in which step(s) a definition or proof strategy is used incorrectly, and describing how the definition or proof strategy was misused.

This proof assumes that the tail element of list L and the element n have the same value. In fact, this statement holds true only when the element being removed is the same as the one being appended. To establish a statement independent of the specific condition where the removed element matches the appended one, we reverse the order of operations between append and removeTail. This ensures that removeTail effectively eliminates whatever append introduces, thereby preserving any element l for all values of n.

Solution To Question 10

(a) Prove or disprove the following statement:

$$\forall l \in L \forall m \in \mathbb{N}(prepend(remove(l, m), m) = l).$$

Solutions: Disproof by counterexample.
Take $l = (1, (2, (3, [])))$ and $m = 4$, the statement evaluates to:

$$\begin{aligned}
LHS &= prepend(remove((1, (2, (3, []))), 4), 4) \\
&= prepend((1, (2, (3, []))), 4) \\
&= (4, (1, (2, (3, [])))) \\
&\neq (1, (2, (3, []))) = l \\
LHS &\neq RHS
\end{aligned}$$

(b) Prove or disprove the following statement:

$$\exists l \in L \exists m \in \mathbb{N}(prepend(remove(l, m), m) = l).$$

Answer: Unlike the previous question that used two $\forall$ quantifiers, this question uses two $\exists$ quantifiers. Already, this statement looks like it has better chances of being true. Let's try to prove the statement with existential generalization. For $l = [1, 2, 3]$ and $m = 1$, the statement equals:

Solutions: Proof by existential generalization, proof by witness.
Take $l = (1, (2, (3, [])))$ and $m = 1$, the statement evaluates to:

$$\begin{aligned}
LHS &= prepend(remove((1, (2, (3, []))), 1), 1) \\
&= prepend((2, (3, [])), 1) \\
&= (1, (2, (3, []))) \\
&= (1, (2, (3, []))) = l \\
LHS &= RHS
\end{aligned}$$

This expression is true, proving there exists some values l and m that cause the expression $(prepend(remove(l, m), m) = l)$ to be true. This proves the original statement through existential generalization. Interestingly, the proposition within the quantifiers will evaluate to true so long as m equals the first (head) element of l.