Math 309 **Summer B 2018**
Homework 5 **Drew Armstrong**

---

1. De Morgan's Law. For all integers $n \geq 1$ let $P(n)$ be the following statement:

"For any n statements $Q_1, Q_2, \ldots Q_n \in \{T, F\}$ we have $\neg(Q_1 \wedge \cdots \wedge Q_n) = \neg Q_1 \vee \cdots \vee \neg Q_n$."

Use induction to prove that $P(n)$ is true for all $n \geq 1$. [Hint: You proved on HW2 that $P(2)$ is a true statement. You do not need to prove this again.]

Proof: The statement $P(1)$ is vacuously true:

"For all $Q \in \{T, F\}$ we have $\neg(Q) = \neg Q$."

And the statement $P(2)$ was proved by you on the second homework:

"For all $Q_1, Q_2 \in \{T, F\}$ we have $\neg(Q_1 \wedge Q_2) = \neg Q_1 \vee \neg Q_2$."

So let us fix an arbitrary integer $k \geq 2$ and let us assume for induction that $P(k)$ is true:

"For all $Q_1, \ldots, Q_k \in \{T, F\}$ we have $\neg(Q_1 \wedge \cdots \wedge Q_k) = \neg Q_1 \vee \cdots \vee \neg Q_k$."

In this hypothetical case we want to show that $P(k+1)$ is also true. For this purpose, let us consider any $k+1$ statements $Q_1, Q_2, \ldots, Q_{k+1} \in \{T, F\}$. Then we have

$$\begin{aligned}
\neg(Q_1 \wedge \cdots \wedge Q_{k+1}) &= \neg\left((Q_1 \wedge \cdots \wedge Q_k) \wedge Q_{k+1}\right) && \text{associativity of } \wedge \\
&= \neg(Q_1 \wedge \cdots \wedge Q_k) \vee \neg Q_{k+1} && P(2) \\
&= (\neg Q_1 \vee \cdots \vee \neg Q_k) \vee \neg Q_{k+1} && P(k) \\
&= \neg Q_1 \vee \cdots \vee \neg Q_{k+1}, && \text{associativity of } \vee
\end{aligned}$$

and hence $P(k+1)$ is true. By the principle of induction we conclude that $P(n)$ is true for all $n \geq 1$. $\square$

2. Euclid's Lemma. Let $p \in \mathbb{Z}$ be prime.

(a) For all integers $a, b \in \mathbb{Z}$ prove that

$$(p|ab) \Rightarrow (p|a \vee p|b).$$

[Hint: It is equivalent to prove $(p|ab \wedge p \nmid a) \Rightarrow p|b$. Use HW3.]

(b) For all integers $n \geq 1$ we define the statement $P(n)$ as follows:

"For any n integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ we have $(p|a_1 a_2 \cdots a_n) \Rightarrow (p|a_i$ for some $i)$."

Use induction to prove that $P(n)$ is true for all $n \geq 1$. [Hint: Part (a) is $P(2)$.]

(a) *Proof:* Let $p \in \mathbb{Z}$ be prime and suppose that $p|ab$ for some $a, b \in \mathbb{Z}$. This means that $pk = ab$ for some $k \in \mathbb{Z}$. In this case we want to prove that either $p|a$ or $p|b$ (or both). So let us suppose for contradiction that $p \nmid a$ and $p \nmid b$.[1] Then since the divisors of p are just ± 1 and $\pm p$, and since p is **not** a divisor of a, we must have $\gcd(p, a) = 1$. It follows from the Extended Euclidean Algorithm that there exist some integers $x, y \in \mathbb{Z}$ such that

$$px + ay = 1.$$

---

[1] By de Morgan's law we know that $\neg(p|a \vee p|b) = (p \nmid a \wedge p \nmid b)$.

Now multiply both sides by b to obtain

$$\begin{aligned} b(px + ay) &= b \\ bpx + (ab)y &= b \\ bpx + (pk)y &= b \\ p(bx + ky) &= b, \end{aligned}$$

which implies that $p|b$. This is the desired contradiction. □

[Remark: It would have been quicker to just quote Problem 4 from Homework 4.]

(b) *Proof:* The statement $P(1)$ is vacuously true:

"For any $a \in \mathbb{Z}$ we have $p|a \Rightarrow p|a$."

And the statement $P(2)$ was proved in part (a):

"For any $a_1, a_2 \in \mathbb{Z}$ we have $(p|a_1a_2) \Rightarrow (p|a_1 \vee p|a_2)$."

So let us fix an arbitrary integer $k \geq 2$ and let us assume for induction that $P(k)$ is true:

"For any $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ we have $(p|a_1a_2\cdots a_k) \Rightarrow (p|a_i$ for some $i)$."

In this hypothetical case we want to show that $P(k+1)$ is also true. For this purpose, let us consider any $k+1$ integers $a_1, a_2, \ldots, a_{k+1} \in \mathbb{Z}$. Then we have

$$\begin{aligned} p|(a_1a_2\cdots a_{k+1}) &= p|(a_1a_2\cdots a_k)a_{k+1} && \text{associativity of } \times \\ &\Rightarrow p|(a_1a_2\cdots a_k) \vee p|a_{k+1} && P(2) \\ &\Rightarrow (p|a_i \text{ for some } 1 \leq i \leq k) \vee p|a_{k+1} && P(k) \\ &= (p|a_1 \vee p|a_2 \vee \cdots \vee p|a_k) \vee p|a_{k+1} && \\ &= (p|a_1 \vee p|a_2 \vee \cdots \vee p|a_{k+1}) && \text{associativity of } \vee \\ &= (p|a_i \text{ for some } 1 \leq i \leq k+1), && \end{aligned}$$

and hence $P(k+1)$ is true. By the principle of induction we conclude that $P(n)$ is true for all $n \geq 1$. □

[Remark: Note that this proof is "exactly the same" as Problem 1. After a while, all proofs by induction start to look exactly the same.]

3. Multiplicative Cancellation. For all integers $n \geq 1$ let $P(n)$ be the following statement:

"$\forall m \geq 1, mn \geq 1$."

(a) Show that $P(1)$ is a true statement.
(b) Consider any integer $k \geq 1$ and assume for induction that $P(k)$ is a true statement. In this case, prove that $P(k+1)$ is also a true statement.
(c) Use the result of (a) and (b) to prove the following:

$$\forall a, b \in \mathbb{Z}, (ab = 0) \Rightarrow (a = 0 \vee b = 0).$$

[Hint: It is equivalent to prove $(a \neq 0 \wedge b \neq 0) \Rightarrow (ab \neq 0)$. If $a \neq 0$ and $b \neq 0$ then we must have $m = |a| \geq 1$ and $n = |b| \geq 1$.]
(d) Use the result of part (c) to prove the following:

$$\forall a, b, c \in \mathbb{Z}, (ab = ac \wedge a \neq 0) \Rightarrow (b = c).$$

(a) The statement $P(1)$ is vacuously true:

"for all integers $m \geq 1$, we have $m \geq 1$."

(b) Consider any integer $k \geq 1$ and assume for induction that $P(k)$ is true, that is:

"for all integers $m \geq 1$, we have $mk \geq 1$."

In this hypothetical case we want to show that $P(k+1)$ is also true, that is:

"for all integers $m \geq 1$, we have $m(k+1) \geq 1$."

So let us consider any integer $m \geq 1$. Then we have

$$\begin{aligned} m(k+1) &= mk + m && \text{distribution} \\ &\geq 1 + m && P(k) \\ &\geq 1, && \text{since } m \geq 1 \end{aligned}$$

and hence $P(k+1)$ is true. By induction, we conclude that $P(n)$ is true for all $n \geq 1$. In other words:

"For all integers $m \geq 1$ and $n \geq 1$, we have $mn \geq 1$."

(c) *Proof:* It is helpful to make the following observation:

if n is a whole number then we have $n \neq 0$ if and only if $|n| \geq 1$.

Now if a, b are any whole numbers, we have

$$\begin{aligned} a \neq 0 \wedge b \neq 0 &\Rightarrow |a| \geq 1 \wedge |b| \geq 1 && \text{observation} \\ &\Rightarrow |a| \cdot |b| \geq 1 && \text{parts (a) and (b)} \\ &\Rightarrow |ab| \geq 1 && \text{since } |a| \cdot |b| = |ab| \\ &\Rightarrow ab \neq 0, && \text{observation} \end{aligned}$$

as desired. □

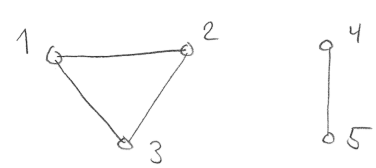
Proof: Consider integers $a, b, c \in \mathbb{Z}$ with $ab = ac$ and $a \neq 0$. Then we have

$$\begin{aligned} ab &= ac \\ ab - ac &= 0 \\ a(b-c) &= 0, \end{aligned}$$

and since $a \neq 0$, the result of part (c) implies that $(b-c) = 0$; in other words, $b = c$. □

[Remark: That was much ado about very little. It might be tempting to just take multiplicative cancellation as part of the **definition** of integers, but no one ever does that. This exercise was to show you that multiplicative cancellation is actually a subtle consequence of induction. Plus, it was just good mind-stretching exercise.]

4. A Graph Theory Problem. A *simple graph* consists of a set V of *vertices*, together with a set E of unordered pairs of vertices, called *edges*. For example, the following graph has $V = \{1,2,3,4,5\}$ and $E = \{\{1,2\},\{2,3\},\{1,3\},\{4,5\}\}$:



We say that a graph is *connected* if for all pairs of vertices $u, v \in V$ there exists some sequence of edges $\{u_1, u_2\}, \{u_2, u_3\}, \ldots, \{u_\ell, u_{\ell+1}\}$ starting with $u_1 = u$ and ending with $u_{\ell+1} = v$. (The graph in the example is **not** connected.)

Use induction to prove that every connected graph with n vertices has at least $n - 1$ edges.

> Hint: For any graph G, let $v(G)$ be its number of vertices and let $e(G)$ be its number of edges. We want to show that every **connected** graph satisfies $e(G) \geq v(G) - 1$. If G is connected, then let us start removing edges as random. At some point (after removing d edges, say) the graph will become disconnected into two connected graphs called G_1 and G_2. Observe that $e(G) = d + e(G_1) + e(G_2)$. How many edges could these smaller graphs have?

Proof by strong induction on the number of vertices: For any **connected graph** G we want to show that

$$\text{“}e(G) \geq v(G) - 1.\text{”}$$

This statement is clearly true when $v(G) = 1$ or $v(G) = 2$. (Think about it.) So let us assume for strong induction that the statement is true for all connected graphs satisfying $v(G) < n$. In this case we want to show that the statement is still true for $v(G) = n$.

So let G be an arbitrary connected graph on n vertices. Start removing edges at random (but keep all the vertices) until the graph becomes disconnected into two pieces G_1 and G_2. Suppose that this happens for the first time after deleting d edges. Then we must have

$$n = v(G) = v(G_1) + v(G_2) \qquad \text{and} \qquad e(G) - d = e(G_1) + e(G_2).$$

But each of the connected graphs G_1, G_2 has **fewer vertices** than G, hence our induction hypothesis implies that

$$e(G_1) \geq v(G_1) - 1 \qquad \text{and} \qquad e(G_2) \geq v(G_2) - 1.$$

Now putting everything together implies that

$$\begin{aligned} e(G) &= e(G_1) + e(G_2) + d \\ &\geq (v(G_1) - 1) + (v(G_2) - 1) + d && \text{induction} \\ &= (v(G_1) + v(G_2)) - 2 + d \\ &= v(G) - 2 + d \\ &\geq v(G) - 1, && \text{since } d \geq 1 \end{aligned}$$

as desired. □

[Remark: I included this problem because a computer science professor told me he wants you to see graph theory in this course. Maybe it was too little, too late. Anyway, I think it was a good final challenge.]