Quiz Section 5: Set Theory, Induction – Solutions

Review

Set theory:

- $A \backslash B = \{x \ : \ x \in A \wedge x \notin B\}$. Or, equivalently, $x \in A \backslash B \leftrightarrow x \in A \wedge x \notin B$.
- $A \times B = \{(a, b) \ : \ a \in A, \ b \in B\}$. Or, equivalently, $(a, b) \in A \times B \leftrightarrow a \in A \wedge b \in B$.
- $\mathcal{P}(A) = \{B \ : \ B \subseteq A\}$. Or, equivalently, $B \in \mathcal{P}(A) \leftrightarrow B \subseteq A$.

5 Steps to an Induction Proof: To prove $\forall n \in \mathbb{N} \ P(n)$ (or equivalently $\forall n \geqslant 0 \ P(n)$ for $n \in \mathbb{Z}$).

1. "Let $P(n)$ be ⟨fill in⟩. We will show that $P(n)$ is true for every $n \in \mathbb{N}$ (or equivalently integer $n \geqslant 0$) by induction."
2. "Base Case:" Prove $P(0)$
3. "Inductive Hypothesis: Suppose $P(k)$ is true for some arbitrary integer $k \geqslant 0$"
4. "Inductive Step:" Prove that $P(k+1)$ is true.

   Use the goal to figure out what you need.
   Make sure you are using I.H. and point out where you are using it.
   (Don't assume $P(k+1)$!)
5. "Conclusion: The claim follows by induction"

Task 1 – Efficient Modular Exponentiation

a) Compute $2^{71} \bmod 25$ using the efficient modular exponentiation algorithm.

$$
\begin{aligned}
2^1 &\equiv 2 \pmod{25} \\
2^2 &\equiv 4 \pmod{25} \\
2^4 &\equiv 16 \pmod{25} \\
2^8 \equiv 16^2 &\equiv 6 \pmod{25} && \text{since } 16^2 \bmod 25 = 256 \bmod 25 = 6 \\
2^{16} \equiv 6^2 &\equiv 11 \pmod{25} \\
2^{32} \equiv 11^2 &\equiv 21 \pmod{25} && \text{since } 11^2 \bmod 25 = 121 \bmod 25 = 21 \\
2^{64} \equiv 21^2 &\equiv 16 \pmod{25} && \text{since } 21^2 \bmod 25 = 441 \bmod 25 = 16
\end{aligned}
$$

Therefore, since $71 = 64 + 4 + 2 + 1$, we see that

$$\begin{aligned} 2^{71} &\equiv 2^{64} \times 2^4 \times 2^2 \times 2^1 \pmod{25} \\ &\equiv 16 \times 16 \times 4 \times 2 \pmod{25} \\ &\equiv 16 \times 16 \times 8 \equiv 16 \times 16 \times 8 \pmod{25} \\ &\equiv 16 \times 128 \equiv 16 \times 3 \pmod{25} \\ &\equiv 48 \equiv 23 \pmod{25} \end{aligned}$$

Therefore $2^{71} \bmod 25 = 23$.

b) How many modular multiplications does the algorithm use for this computation?

6 to compute $2^k \bmod 71$ for k a power of 2 plus 3 to multiply the ones selected for the final result $= 9$.

Task 2 – How Many Elements?

For each of these, how many elements are in the set? If the set has infinitely many elements, say ∞.

a) $A = \{1, 2, 3, 2\}$

3

b) $B = \{\{\},\ \{\{\}\},\ \{\{\}, \{\}\},\ \{\{\}, \{\}, \{\}\},\ \dots\}$

$$\begin{aligned} B &= \{\{\},\ \{\{\}\},\ \{\{\}, \{\}\},\ \{\{\}, \{\}, \{\}\},\ \dots\} \\ &= \{\{\},\ \{\{\}\},\ \{\{\}\},\ \{\{\}\},\ \dots\} \\ &= \{\varnothing, \{\varnothing\}\} \end{aligned}$$

So, there are two elements in B.

c) $D = \varnothing$

0.

d) $E = \{\varnothing\}$

1.

e) $C = A \times (B \cup \{7\})$

$C = \{1, 2, 3\} \times \{\varnothing, \{\varnothing\}, 7\} = \{(a, b) \mid a \in \{1, 2, 3\}, b \in \{\varnothing, \{\varnothing\}, 7\}\}$. It follows that there are $3 \times 3 = 9$ elements in C.

f) $G = \mathcal{P}(\{\varnothing\})$

$2^1 = 2$. The elements are $G = \{\varnothing, \{\varnothing\}\}$.

Task 3 – Set Replay

Prove each of the following set identities.

a) $A\backslash B \subseteq A \cup C$ for any sets A, B, C.

Let x be an arbitrary object. Suppose that $x \in A\backslash B$. By definition, this means that $x \in A$ and $x \notin B$. Since $x \in A$, we have $x \in A \cup C$ by the definition of $\cup$. Since x was arbitrary, this shows $A\backslash B \subseteq A \cup C$.

b) $(A\backslash B)\backslash C \subseteq A\backslash C$ for any sets A, B, C.

Let x be an arbitrary object. Suppose that $x \in (A\backslash B)\backslash C$. By definition, this means that $x \in A\backslash B$ and $x \notin C$ and then that $x \in A$ and $x \notin B$. The facts that $x \in A$ and $x \notin C$ show that $x \in A\backslash C$ by definition. Since x was arbitrary, this shows $(A\backslash B)\backslash C \subseteq A\backslash C$.

c) $(A \cap B) \times C \subseteq A \times (C \cup D)$ for any sets A, B, C, D.

Let x be an arbitrary element of $(A \cap B) \times C$. Then, by definition of Cartesian product, x must be of the form (y, z) where $y \in A \cap B$ and $z \in C$. Since $y \in A \cap B$, by definition of $\cap$, $y \in A$ (and $y \in B$). Since $z \in C$, by definition of $\cup$, we also have $z \in C \cup D$. Thus, since $y \in A$ and $z \in C \cup D$, by definition of Cartesian product we have $x = (y, z) \in A \times (C \cup D)$. Since x was an arbitrary element of $(A \cap B) \times C$ we have proved that $(A \cap B) \times C \subseteq A \times (C \cup D)$ as required.

Task 4 – Set Equality

Let A and B be sets. Consider the claim: $A\backslash(B \cup C) = (A\backslash B) \cap (A\backslash C)$.
State what the claim becomes when you unroll the definition of "=" sets. Then, following the Meta Theorem template, write an English proof that the claim holds.

Unrolling the $=$, the claim is: $\forall x((x \in A\backslash(B \cup C)) \leftrightarrow (x \in (A\backslash B) \cap (A\backslash C)))$.

Let x be arbitrary.

$$
\begin{aligned}
x \in A\backslash(B \cup C) &\equiv x \in A \wedge \neg(x \in (B \cup C)) && \text{[Def of Set Difference]} \\
&\equiv x \in A \wedge \neg(x \in B \vee x \in C) && \text{[Def of Union]} \\
&\equiv x \in A \wedge (x \notin B \wedge x \notin C) && \text{[De Morgan]} \\
&\equiv (x \in A \wedge x \in A) \wedge (x \notin B \wedge x \notin C) && \text{[Idempotency]} \\
&\equiv (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) && \text{[Associativity/Commutativity]} \\
&\equiv (x \in (A\backslash B)) \wedge (x \in (A\backslash C)) && \text{[Def of Set Difference]} \\
&\equiv (x \in (A\backslash B) \cap (A\backslash C)) && \text{[Def of Intersection]}
\end{aligned}
$$

Since x was arbitrary, we have shown that the two sets contain the same elements.

Task 5 – Power Sets

Let A and B be sets. Prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ follows from $A \subseteq B$.

Let X be an arbitrary set in $\mathcal{P}(A)$. By definition of power set, $X \subseteq A$. We need to show that $X \in \mathcal{P}(B)$, or equivalently, that $X \subseteq B$.

Let x be an arbitrary element of X. Since $X \subseteq A$, it must be the case that $x \in A$. We were given that $A \subseteq B$. By definition of subset, any element of A is an element of B. So, it must also be the case that $x \in B$.

Since x was arbitrary, we know any element of X is an element of B. By definition of subset, $X \subseteq B$. By definition of power set, $X \in \mathcal{P}(B)$.

Since X was an arbitrary set, any set in $\mathcal{P}(A)$ is in $\mathcal{P}(B)$, or, by definition of subset, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. We have shown the claim.

Task 6 – Beset with Power

Show that for any set X and any set A such that $A \in \mathcal{P}(X)$, there exists a set $B \in \mathcal{P}(X)$ such that $A \cap B = \varnothing$ and $A \cup B = X$.

The approach to this problem is less direct than some others. The solution will cover both the answer and the intuition used to arrive at it.

In this solution we first explain the intuition and the strategy we take before giving the proof.

We start by letting X and A be arbitrary sets and assume that $A \in \mathcal{P}(X)$. We first think about how to express this more simply. By definition of power set, this means $A \subseteq X$ which is simpler to understand.

Now we think about our goal. We want to show there is some set B with the given properties. There are three of them:

- We must have $B \in \mathcal{P}(X)$ which means that $B \subseteq X$.
- We must have $A \cap B = \varnothing$.
- We must have $A \cup B = X$.

The last two properties say that B can't contain anything that is in A and that the elements of B together with those in A must give all elements of X. That is, B must consist precisely those elements of X that aren't in A. In other words, we must have $B = X \backslash A$. It seems that it will work for all three properties.

Now here's the proof:
Let X and A be arbitrary sets and assume that $A \in \mathcal{P}(X)$.Define $B = X \backslash A$. Let x be an arbitrary object. By definition,

$$x \in B \equiv x \in X \backslash A \equiv (x \in X \wedge x \notin A),$$

so $x \in B$ implies that $x \in X$. Therefore $B \subseteq X$ and hence $B \in \mathcal{P}(X)$.
Furthermore $x \in B$ implies $\neg(x \in A)$ and hence $A \cap B = \varnothing$.
Finally, since $A \subseteq X$, we have $A \cup (X \backslash A) = X$ and hence $A \cup B = X$. This last statement does need the assumption about A so we give the detailed proof below:

$$\begin{aligned} x \in A \cup B &\equiv x \in A \cup (X \backslash A) \\ &\equiv (x \in A) \vee ((x \in X \wedge \neg(x \in A)) \\ &\equiv ((x \in A) \vee (x \in X)) \wedge ((x \in A) \vee \neg(x \in A)) \\ &\equiv (x \in X) \wedge \mathbf{T} \qquad \textbf{since } A \subseteq X \\ &\equiv x \in X. \end{aligned}$$

Thus $A \cup B = X$ and hence B satisfies all the three required properties which proves the claim.

Task 7 – Induction with Equality

a) Define the triangle numbers as $\triangle_n = 0 + 1 + 2 + \cdots + n$, where $n \in \mathbb{N}$. In class we showed $\triangle_n = \frac{n(n+1)}{2}$.

Prove the following equality for all $n \in \mathbb{N}$:

$$0^3 + 1^3 + \cdots + n^3 = \triangle_n^2$$

First, note that $\triangle_n = (0 + 1 + 2 + \cdots + n)$. So, we are trying to prove

$$(0^3 + 1^3 + \cdots + n^3) = (0 + 1 + \cdots + n)^2$$

Proof: Let $P(n)$ be the statement:

$$0^3 + 1^3 + \cdots + n^3 = (0 + 1 + \cdots + n)^2.$$

We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case. $0^3 = 0^2$, so $P(0)$ holds.

Inductive Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$.

Inductive Step. We show $P(k+1)$:

$$\begin{aligned}
0^3 + 1^3 + \cdots (k+1)^3 &= (0^3 + 1^3 + \cdots + k^3) + (k+1)^3 && \text{[Associativity]} \\
&= (0 + 1 + \cdots + k)^2 + (k+1)^3 && \text{[Inductive Hypothesis]} \\
&= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 && \text{[Proved in class]} \\
&= (k+1)^2 \left(\frac{k^2}{2^2} + (k+1)\right) && \text{[Factor } (k+1)^2\text{]} \\
&= (k+1)^2 \left(\frac{k^2 + 4k + 4}{4}\right) && \text{[Add via common denominator]} \\
&= (k+1)^2 \left(\frac{(k+2)^2}{4}\right) && \text{[Factor numerator]} \\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2 && \text{[Take out the square]} \\
&= (0 + 1 + \cdots + (k+1))^2 && \text{[Formula from class again]}
\end{aligned}$$

Conclusion: $P(n)$ is true for all $n \in \mathbb{N}$ by the principle of induction.

b) For every $n \in \mathbb{N}$, define S_n to be the sum of the squares of the natural numbers up to n, or

$$S_n = 0^2 + 1^2 + \cdots n^2.$$

For all $n \in \mathbb{N}$, prove that $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be the statement "$S_n = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case. $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)((2)(0)+1) = 0$, we know that P(0) is true.

Induction Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$.

Induction Step. Examining S_{k+1}, we see that

$$S_{k+1} = 0^2 + 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = S_k + (k+1)^2.$$

By the induction hypothesis, we know that $S_k = \frac{1}{6}k(k+1)(2k+1)$. Therefore, we can substitute and rewrite the expression as follows:

$$\begin{aligned}
S_{k+1} &= S_k + (k+1)^2 && \text{by definition} \\
&= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by the I.H.} \\
&= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right) && \text{using common factor } (k+1) \\
&= \frac{1}{6}(k+1)\left(k(2k+1) + 6(k+1)\right) \\
&= \frac{1}{6}(k+1)\left(2k^2 + 7k + 6\right) \\
&= \frac{1}{6}(k+1)(k+2)(2k+3) && \text{factoring the quadratic term} \\
&= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}$$

Thus, we can conclude that $P(k+1)$ is true.

Note: We used the fact that we needed to prove $P(k+1)$ as a clue to help us figure out what the factors of that quadratic term might be. If $P(k+1)$ had not been correct then this wouldn't have worked out.

Conclusion: Therefore, $P(n)$ is true for all $n \in \mathbb{N}$ by induction.

Task 8 – Induction with Divides

Prove that $9 \mid (n^3 + (n+1)^3 + (n+2)^3)$ for all $n > 1$ by induction.

Let $P(n)$ be "$9 \mid n^3 + (n+1)^3 + (n+2)^3$". We will prove $P(n)$ for all integers $n > 1$ by induction.

Base Case $(n = 2)$**:** $2^3 + (2+1)^3 + (2+2)^3 = 8 + 27 + 64 = 99 = 9 \cdot 11$, so $9 \mid 2^3 + (2+1)^3 + (2+2)^3$, so $P(2)$ holds.

Induction Hypothesis: Assume that $9 \mid j^3 + (j+1)^3 + (j+2)^3$ for an arbitrary integer $j > 1$. Note that this is equivalent to assuming that $j^3 + (j+1)^3 + (j+2)^3 = 9k$ for some integer k by the definition of divides.

Induction Step: Goal: Show $9 \mid (j+1)^3 + (j+2)^3 + (j+3)^3$

$$\begin{aligned}(j+1)^3 + (j+2)^3 + (j+3)^3 &= (j+3)^3 + 9k - j^3 \text{ for some integer } k && \text{[Induction Hypothesis]}\\ &= j^3 + 9j^2 + 27j + 27 + 9k - j^3\\ &= 9j^2 + 27j + 27 + 9k\\ &= 9(j^2 + 3j + 3 + k)\end{aligned}$$

Since j is an integer, $j^2 + 3j + 3 + k$ is also an integer. Therefore, by the definition of divides, $9 \mid (j+1)^3 + (j+2)^3 + (j+3)^3$, so $P(j) \to P(j+1)$ for an arbitrary integer $j > 1$.

Conclusion: $P(n)$ holds for all integers $n > 1$ by induction.

Task 9 – Induction with Inequality

Prove that $6n + 6 < 2^n$ for all $n \geqslant 6$.

Let $P(n)$ be "$6n + 6 < 2^n$". We will prove $P(n)$ for all integers $n \geqslant 6$ by induction on n

Base Case $(n = 6)$**:** $6 \cdot 6 + 6 = 42 < 64 = 2^6$, so $P(6)$ holds.

Inductive Hypothesis: Assume that $6k + 6 < 2^k$ for an arbitrary integer $k \geqslant 6$.

Inductive Step: Goal: Show $6(k+1) + 6 < 2^{k+1}$

$$\begin{aligned}6(k+1) + 6 &= 6k + 6 + 6\\ &< 2^k + 6 && \text{[Inductive Hypothesis]}\\ &< 2^k + 2^k && \text{[Since } 2^k > 6\text{, since } k \geqslant 6\text{]}\\ &= 2 \cdot 2^k\\ &= 2^{k+1}\end{aligned}$$

So $P(k) \to P(k+1)$ for an arbitrary integer $k \geqslant 6$.

Conclusion: $P(n)$ holds for all integers $n \geqslant 6$ by the principle of induction.

Task 10 – A Horse of a Different Color

Did you know that all dogs are named Dubs? It's true. Maybe. Let's prove it by induction. The key is talking about groups of dogs, where every dog has the same name.

Let $P(i)$ mean "all groups of i dogs have the same name." We prove $\forall n\ P(n)$ by induction on n.

Base Case: $P(1)$ Take an arbitrary group of one dog, all dogs in that group all have the same name (there's only the one, so it has the same name as itself).

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary k.

Inductive Step: Consider an arbitrary group of $k+1$ dogs. Arbitrarily select a dog, D, and remove it from the group. What remains is a group of k dogs. By inductive hypothesis, all k of those dogs have the same name. Add D back to the group, and remove some other dog D'. We have a (different) group of k dogs, so the inductive hypothesis applies again, and every dog in that group also shares the same name. All $k+1$ dogs appeared in at least one of the two groups, and our groups overlapped, so all of our $k+1$ dogs have the same name, as required.

Conclusion: We conclude $P(n)$ holds for all n by the principle of induction.

Recalling that Dubs is a dog, we have that every dog must have the same name as him, so every dog is named Dubs.

This proof cannot be correct (the proposed claim is false). Where is the bug?

The bug is in the final sentence of the inductive step. We claimed that the groups overlapped, i.e. that some dog was in both of them. That's true for large k, but not when $k+1=2$. When $k=2$, D is in a group by itself, and D' was in a group by itself. The inductive hypothesis holds (D has the only name in its subgroup, and D' has the only name in its subgroup) but returning to the full group $\{D, D'\}$ we cannot conclude that they share a name.

From there everything unravels. $P(1) \nrightarrow P(2)$, so we cannot use the principle of induction. It turns out this is the **only** bug in the proof. The argument in the inductive step is correct as long as $k+1>2$. But that implication is always vacuous, since $P(2)$ is false.

In fact, if you think about it in common English, every pair of dogs having the same name (which is exactly what $P(2)$ says), is equivalent to saying that all dogs have the same name.