Quiz Section 5: Set Theory, Induction

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.

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

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

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

c) $D = \varnothing$

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

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

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

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.

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

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

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.

Task 5 – Power Sets

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

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.

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 $n \in \mathbb{N}$:

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

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 $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Task 8 – Induction with Divides

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

Task 9 – Induction with Inequality

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

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?