CS1231S: Discrete Structures

Tutorial #7: Mathematical Induction and Recursion

(Week 9: 14 – 18 October 2024)

I. Discussion Questions

These are meant for you to discuss on Canvas. No answers will be provided.

> **Definition:**
> An integer d is said to be a **linear combination** of integers a and b, if and only if, there exist integers s and t such that $as + bt = d$.

D1. Prove the following proposition:

$$\forall a, b, c \in \mathbb{Z}, \text{ if } a \mid b \text{ and } a \mid c, \text{ then } \forall x, y \in \mathbb{Z}\ (a \mid bx + cy).$$

The proposition states that if a divides both b and c, then a divides their linear combination.

D2. Aiken attempts to prove the following by Mathematical Induction:

$$\forall n \in \mathbb{N}\ \big(3 \mid (n^3 + 44n)\big).$$

However, his proof below is incorrect. Point out the mistakes.

Proof:

1. Note that $1^3 + 44(1) = 45$ which is divisible by 3.
2. So the statement is true for $n = 1$.
3. Now suppose the statement is true for some natural number k.
4. Then $k^3 + 44k$ is divisible by 3.
5. Therefore $(k+1)^3 + 44(k+1)$ is divisible by 3.
6. So by Mathematical Induction, the statement is true for all numbers.

D3. Dueet attempts to prove the following by Mathematical Induction.

Consider a group of n people, each of whom shakes hands exactly once with everybody else in the group. No one shakes his/her own hand. Let $S(n)$ be the total number of handshakes in any group of n people. Prove that

$$\forall n \in \mathbb{Z}^+ \left(S(n) = \frac{n(n-1)}{2}\right).$$

However, her proof below is incorrect. Point out the mistake.

Proof:

1. Let $P(n) \equiv (S(n) = \frac{n(n-1)}{2})$, for any $n \in \mathbb{Z}^+$.
2. Basis step: $n = 1$
   2.1. $S(1) = 0$ because nobody shakes his/her own hand.
   2.2. Also, $\frac{1(1-1)}{2} = 0 = S(1)$.
   2.3. Thus $P(1)$ is true.
3. Inductive step: Assume $P(k)$, i.e. $S(k) = \frac{k(k-1)}{2}$.
   3.1. For any $k \in \mathbb{Z}^+$, consider any group of k people.
   3.2. This group makes $S(k)$ handshakes, by the inductive hypothesis.
   3.3. Now consider one new person joining the group. Since all the original k people have already shaken hands, they just need to shake the newcomer's hand, giving k additional handshakes in total.
   3.4. Thus $S(k+1) = S(k) + k = \frac{k(k-1)}{2} + k = \frac{(k+1)k}{2}$ by basic algebra.
   3.5. Hence $P(k+1)$ is true.
4. Therefore $P(n)$ is true for any $n \in \mathbb{Z}^+$, by mathematical induction.

II. Tutorial Questions

In writing Mathematical Induction proofs, please follow the format we use in class.

1. Many common mistakes are spotted in Mathematical Induction proofs. For each of the following, point out the mistake. (If you follow the format we introduced in class, it will help you avoid making some of these mistakes.)

   Consider this problem: Prove by mathematical induction that for all $n \in \mathbb{Z}^+$,

   $$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

   Define the statement $P(n)$ to be "$1 + 2 + \cdots n = n(n+1)/2$".

   (a) Inductive hypothesis: Assume that $P(k)$ is true.
   Inductive step: $\sum_{i=1}^{k+1} i = (k+1) + \sum_{i=1}^{k} i = (k+1) + P(k) = \cdots$

   (b) Inductive step:
   1. $1 + 2 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2}$
   2. Hence $\frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$ (by the inductive hypothesis)
   3. Hence $\frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$ (by basic algebra)
   4. Hence $\frac{(k+1)(k+2)}{2} = \frac{(k+1)(k+2)}{2}$.
   5. Since (4) is a tautology, (1) must be true.

   (c) Inductive hypothesis: Assume that $P(k)$ is true for all $k \in \mathbb{Z}^+$.

2. Prove by induction that for all $n \in \mathbb{Z}^+$,
$$\mathbf{1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1).}$$

3. Let $x \in \mathbb{R}_{\geq -1}$. Prove by induction that $\mathbf{1 + nx \leq (1+x)^n}$ for all $n \in \mathbb{Z}^+$.

4. Let a be an odd integer. Prove by induction that $\mathbf{2^{n+2} \mid (a^{2^n} - 1)}$ for all $n \in \mathbb{Z}^+$.
Here you may use without proof the fact that the product of any two consecutive integers is even. (Prove that as your own exercise – it's very simple.)
(Note that $a^{b^c} = a^{(b^c)}$ by convention.)

5. Prove by induction that
$$\forall \boldsymbol{n} \in \mathbb{Z}_{\geq \mathbf{8}}\ \exists \boldsymbol{x}, \boldsymbol{y} \in \mathbb{N}\ (\boldsymbol{n} = \mathbf{3}\boldsymbol{x} + \mathbf{5}\boldsymbol{y}).$$
(In other words, any integer-valued transaction of at least $8 can be carried out using only $3 and $5 notes.)

6. Prove by induction that every positive integer can be written as a sum of *distinct* non-negative integer powers of 2, i.e.,
$$\forall \boldsymbol{n} \in \mathbb{Z}^+\ \exists \boldsymbol{l} \in \mathbb{Z}^+\ \exists \boldsymbol{i_1}, \boldsymbol{i_2}, \cdots, \boldsymbol{i_l} \in \mathbb{N}\ (\boldsymbol{i_1} < \boldsymbol{i_2} < \cdots < \boldsymbol{i_l}\ \wedge \boldsymbol{n} = \mathbf{2}^{\boldsymbol{i_1}} + \mathbf{2}^{\boldsymbol{i_2}} + \cdots + \mathbf{2}^{\boldsymbol{i_l}}).$$

7. Let $a_0, a_1, a_2 \cdots$ be the sequence satisfying
$$a_0 = 0, \quad a_1 = 2, \quad a_2 = 7, \quad \text{and} \quad a_{n+3} = a_{n+2} + a_{n+1} + a_n$$
for all $n \in \mathbb{N}$. Prove by induction that $\boldsymbol{a_n} < \mathbf{3}^{\boldsymbol{n}}$ for all $n \in \mathbb{N}$.

8. [Adapted from AY2023/24 Semester 1 exam]
Consider the Fibonacci function:
$$F(0) = 0; \qquad F(1) = 1; \qquad F(n+1) = F(n) + F(n-1), n \geq 1.$$
One interesting property of this function can be expressed as follows:
$$P(a,b) \equiv F(a+b) = \big(F(a+1) \times F(b) + F(a) \times F(b-1)\big),\ \forall a \geq 0, b \geq 1.$$
In your proofs for the parts below, you may use "basic algebra" for identity/commutative/associative laws of addition and multiplication, but if the distributive law is used, you must state it explicitly.
   (a) There are a few induction schemes possible to solve part (b). For this question, use the following basis steps: $P(0,b)$ and $P(1,b)$, for all $b \geq 1$. Prove these basis steps.
   (b) Let $b \in \mathbb{N}$. Prove that
   $$P(n-1,b) \wedge P(n,b) \rightarrow P(n+1,b) \text{ for all } n \in \mathbb{Z}^+.$$

9. The set H of Hamming numbers is recursively defined as follows.

   (1) $1 \in H$. (base clause)

   (2) If $n \in H$, then $2n \in H$ and $3n \in H$ and $5n \in H$ (recursion clause)

   (3) Membership for H can always be demonstrated by (finitely many) successive applications of clauses above. (minimality clause)

   A proof rule using regular induction for this set of Hamming numbers can be written as:

   $$P(1)$$
   $$\forall n \in H\ \big(P(n) \Rightarrow P(2n) \wedge P(3n) \wedge P(5n)\big)$$
   $$\therefore\ \forall n \in H\ P(n)$$

   Use this 1PI proof rule/axiom, to show that Hamming numbers have a canonical representation.

   A set has a **canonical representation** if there is a unique way for representing each distinct member of the set. For example, the Hamming number built by the following three ways

   $$2 \times \big(3 \times (3 \times 1)\big) \text{ or } 3 \times \big(2 \times (3 \times 1)\big) \text{ or } 3 \times \big(3 \times (2 \times 1)\big)$$

   are equivalent to each other. Fortunately, we can represent Hamming numbers from this equivalent class of numbers in a canonical/unique manner by writing $2^1 3^2 5^0$.

   We can prove that a canonical representation exists for H by proving the following property:

   $$P(n) \equiv \exists!\, i\ \exists!\, j\ \exists!\, k\ \Big((i, j, k \geq 0) \wedge n = 2^i 3^j 5^k\Big)$$

   Use 1PI to prove that this canonical representation exists for H.

10. Define a set S recursively as follows.

    (1) $2 \in S$. (base clause)

    (2) If $x \in S$, then $3x \in S$ and $x^2 \in S$. (recursion clause)

    (3) Membership for S can always be demonstrated by (finitely many) successive applications of clauses above. (minimality clause)

    Which of the numbers $0, 6, 15, 16, 36$ are in S? Which are not?

11. Let $A = \{1,2,3,4,5\}$ and $B = \{1,3,5,7,9\}$. Define a set S recursively as follows.

    (1) $A, B \in S$. (base clause)

    (2) If $X, Y \in S$, then $X \cap Y \in S$ and $X \cup Y \in S$ and $X \setminus Y \in S$ (recursion clause)

    (3) Membership for S can always be demonstrated by (finitely many) successive applications of clauses above. (minimality clause)

    For each of the following sets, determine whether it is in S, and use one sentence to explain your answer.

    (a) $C = \{2,4,7,9\}$.

    (b) $D = \{2,3,4,5\}$.