CS 30: Discrete Math in CS (Winter 2019): Lecture 14

Date: 28th January, 2019 (Monday)
Topic: Principle of Mathematical Induction
Disclaimer: These notes have not gone through scrutiny and in all probability contain errors.
Please discuss in Piazza/email errors to deeparnab@dartmouth.edu

1. **Formal Setting.**

   Mathematical Induction is used to prove theorems of the form $\forall n \in \mathbb{N} : \ P(n)$ where P is some predicate with the natural numbers as the domain of discourse. Formally, it is stated as follows
   $$\Big(P(1) \wedge (\forall k \in \mathbb{N} : P(k) \Rightarrow P(k+1))\Big) \Rightarrow (\forall n \in \mathbb{N} : P(n)) \tag{PMI}$$
   In plain English, it asserts that to prove the statement "$P(n)$ is true for all $n \in \mathbb{N}$.", it suffices to prove

   - **The Base Case:**(*often easy*) Prove that $P(0)$ is true; and
   - **The Inductive Case:**(*the meat!*) For any natural number k, if $P(k)$ is true, then prove that $P(k+1)$ is true.

   In the inductive case, the *assumption* that "$P(k)$ is true" is called the Induction Hypothesis.

2. **Meeting an old friend.**

   Let us use induction to prove something we proved in the first class.

   Theorem 1. For all non-negative integers n, $\sum_{i=1}^{n} i = n(n+1)/2$

   The predicate $P(n)$ takes the value true if $\sum_{i=1}^{n} i = n(n+1)/2$ and false otherwise. (1) asserts that $P(n)$ is true for all natural numbers.

   Proof. To prove $\forall n \in \mathbb{N} : P(n)$, the principle of mathematical induction (or simple induction, henceforth) asks us to check/prove the following.

   Base Case: Let us verify that $P(1)$ is true. Indeed, $\sum_{i=1}^{1} i = 1$ and $\frac{1(1+1)}{2} = 1$, and thus $P(1)$ is true.

   Inductive Case: Fix any natural number k. The induction hypothesis is that $P(k)$ is true. We need to prove $P(k+1)$ is true.

   $P(k)$ is true implies
   $$\sum_{i=1}^{k} i = \frac{k(k+1)}{2} \tag{Induction Hypothesis}$$
   To prove $P(k+1)$ is true, that is, we need to show
   $$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2} \tag{Need to Show}$$

We establish this by noting that the LHS of (Need to Show) is

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1) = (k+1) \cdot \left(\frac{k}{2} + 1\right) = \frac{(k+1)(k+2)}{2}$$

where in the second inequality we have used the (Induction Hypothesis). Thus, we have established (Need to Show), and thus $\forall n \in \mathbb{N} : P(n)$ follows from induction. □

Exercise: *Using induction, prove*

- $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ *for any non-negative integer* n.
- $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$ *for any non-negative integer* n.
- $\sum_{i=1}^{n} a^i = \frac{a^{n+1}-1}{a-1}$ *for any integer* $a > 1$ *and non-negative integer* n.

3. **A Divisibility Fact.** We now prove the following fact by induction.

Theorem 2. For all $n \in \mathbb{N}$, 3 divides $n^3 - n$.

Proof. Let $P(n)$ be the predicate representing the truth value of the statement given in the theorem for a fixed natural number n. We proceed to prove $\forall n \in \mathbb{N} : P(n)$ by induction.

Base Case: Let us verify $P(1)$. We need to verify that 3 divides $1^3 - 1 = 0$. Indeed, 3 times 0 is 0.

Inductive Case: Let us now assume for a *fixed* $k \in \mathbb{N}$ that $P(k)$ is true. That is, 3 divides $k^3 - k$. We need to show $P(k+1)$ is true, that is, 3 divides $(k+1)^3 - (k+1)$. To do so, we expand $(k+1)^3$, to get

$$(k+1)^3 - (k+1) = (k^3 + 3k^2 + 3k + 1) - (k+1) = (k^3 - k) + 3(k^2 + k)$$

$3(k^2 + k)$ is divisible by 3, and by the *induction hypothesis* (that is, $P(k)$ is true), $k^3 - k$ is divisible by 3. Therefore, $(k+1)^3 - (k+1)$ is divisible by 3. That is, $P(k+1)$ is true. By the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

Remark: *But you already knew the above fact, right? Note that* $n^3 - n = n \cdot (n^2 - 1)$. *If* $n \equiv 0 \mod 3$, *then* $n^3 - n$ *is divisible by* 3. *Otherwise, since* 3 *is prime, Fermat's Little Theorem says* $n^2 - 1 \equiv_0 3$, *and thus* $n^3 - n$ *is divisible by* 3. *It is good to prove the same theorem in more than one ways.*

Exercise: *Does* 4 *divide* $n^4 - n$ *for all non-negative integers* n? *Does* 5 *divide* $n^5 - n$ *for all non-negative integers* n?

4. **Another Divisibility Fact.** We now prove the following fact by induction.

Theorem 3. For all $n \in \mathbb{N}$, 7 divides $3^{2n} - 2^n$.

Proof. Let $P(n)$ be the predicate representing the truth value of the statement given in the theorem for a fixed natural number n. We proceed to prove $\forall n \in \mathbb{N} : P(n)$ by induction.

Base Case: Let us verify $P(1)$. We need to verify that 7 divides $3^2 - 2^1 = 7$. Indeed it does. Therefore $P(1)$ is true.

Inductive Case: Let us now assume for a *fixed* $k \in \mathbb{N}$ that $P(k)$ is true. That is, 7 divides $3^{2k} - 2^k$. We need to show $P(k+1)$ is true, that is, 7 divides $3^{2(k+1)} - 2^{(k+1)}$. Indeed observe,

$$\begin{aligned}
3^{2(k+1)} - 2^{(k+1)} &= 3^2 \cdot 3^{2k} - 2 \cdot 2^k \\
&= 9 \cdot 3^{2k} - 2 \cdot 2^k \\
&= 9 \cdot 3^{2k} - 9 \cdot 2^k + 9 \cdot 2^k - 2 \cdot 2^k \qquad (1) \\
&= 9 \cdot \left(3^{2k} - 2^k\right) + 7 \cdot 2^k \qquad (2)
\end{aligned}$$

7 divides $3^{2k} - 2^k$, by the induction hypothesis. 7 clearly divides $7 \cdot 2^k$. Therefore, 7 divides $3^{2(k+1)} - 2^{k+1}$. That is, $P(k+1)$ is true. By the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$.

This proof was (slightly) tricky. Line 1 is where the trick was where we subtracted and added $9 \cdot 2^k$. Why did we do that? Well, we knew something about $3^{2k} - 2^k$, but when we expanded out we got $9 \cdot 3^{2k} - 2 \cdot 2^k$. If the "coefficients" of 3^{2k} and 2^k were same we would be done (but it isn't), so we just added and subtracted so that the coefficients of one became the same. The other we had an "happy accident" (of $9 - 2 = 7$). Indeed, the person who devised this theorem (in this case, me) probably worked backwards to come up with the statement. □

Exercise: *Can you come up with statements like above? Can you guess which number will always divide $4^{3n} - 3^{2n}$ for all natural numbers n? After guessing, can you prove that guess using induction.*

5. **Proving Recursive Programs Correct.** Induction *is* the way to prove recursive programs correct. For example, consider the following program.

```
procedure FACT($n$) ▷ Assume $n \in \mathbb{N}$.
    if $n = 1$ then:
        return 1
    else:
        return $n \cdot$FACT($n - 1$)
```

We now prove the following

Theorem 4. For all positive integers n, $\textsc{Fact}(n)$ returns n!

Proof. We prove by induction the statement $\forall n \in \mathbb{N} : P(n)$, where $P(n)$ is the predicate $\textsc{Fact}(n)$ returns $n!$.

Base Case: Let us verify $P(1)$. By definition of the factorial function, $1! = 1$. Now, if $n = 1$, then Line (3) returns 1. Thus, the base case is verified; $P(1)$ is indeed true.

Inductive Case: Let us now assume for a *fixed* $k \in \mathbb{N}$ that $P(k)$ is true. That is $\textsc{Fact}(k)$ indeed returns $k!$. We need to prove $P(k+1)$, that is, we need to prove $\textsc{Fact}(k+1)$ returns $(k+1)!$.

Inspecting Line (5), we see that $\textsc{Fact}(k+1)$ returns $(k+1)$ times the number returned by $\textsc{Fact}(k)$. By the induction hypothesis, the latter number is $k!$. Therefore, $\textsc{Fact}(k+1)$ returns $(k+1) \cdot k! = (k+1)!$. Therefore, the inductive case is true, and so by induction, the theorem is proved. □

Remark: *Sometimes, the induction principle may look as follows: (a) The base case may involve proving $P(1), P(2), \ldots, P(c)$ for some finite c, and (b) The inductive case may be possible only for numbers $k \geq c$. Note this is also perfectly OK to establish $\forall n : P(n)$. We will see such an example in class and problem sets.*