CS 30: Discrete Math in CS (Winter 2019): Lecture 15

Date: 30th January, 2019 (Wednesday)

Topic: Strong 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. **Making Life Easier.**

   In the inductive case mentioned last time, we needed to show $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$ is true. It actually suffices to prove an easier statement.

   - **Base Case:** $P(1)$ is true; and
   - **Inductive Case:** For all $n \in \mathbb{N}$, if $P(n), P(n-1), \ldots, P(1)$ is true (em induction hypothesis), then $P(n+1)$ is true,

   then, $P(n)$ is true for all $n \in \mathbb{N}$.

   Since we assume more things to prove the same thing, the above is often easier to establish. This way of proving is often called ***strong induction.***

   > **Remark:** *Personally, I am not a big fan of these different names. In my day-to-day life, I call both of these methods (and the others that are coming) just plain induction. But if it helps you, please make the distinction. I will try to do so in class.*

2. **Prime Factorization.**

   > **Theorem 1.** Every natural number ≥ 2 can be written as a product of primes.

   Proof. Let $P(n)$ be the predicate which takes the value true if the number n can be written as a product of primes. We need to prove $\forall n \in \mathbb{N}, n \geq 2 : P(n)$. We proceed by induction.

   Base Case: Note that the base case is $P(2)$ (and not $P(1)$ since that is not asserted to be true). Indeed 2 can be written as a product of primes; therefore $P(2)$ is true.

   Inductive Case: Fix a natural number $k \geq 2$. Assume $P(k), P(k-1), \ldots, P(2)$ are all true. We need to establish $P(k+1)$. That is, we need to prove $(k+1)$ can be written as a product of primes.

   Case 1: $(k+1)$ is a prime. In this case, there is nothing to show; $(k+1)$ is a product of the single prime $(k+1)$.

   Case 2: $(k+1)$ is *not* a prime. This implies, there exists two natural numbers a and b such that (i) $2 \leq a \leq k$ and $2 \leq b \leq k$, and (ii) $(k+1) = a \cdot b$.

   By the inductive hypothesis, $P(a)$ and $P(b)$ are both true (note, the "weak" induction wouldn't have told us this). Therefore, a can be written as product of primes, and b can be written as a product of primes, and therefore, $a \cdot b$ can be written as a product of primes. That is, $(k+1)$ can be written as a product of primes. We have therefore established $P(k+1)$ is true.

   By (strong) induction, therefore, $\forall n \geq 2, n \in \mathbb{N} : P(n)$ is true. ☐

Remark: *Does the theorem above prove that every natural number* ≥ 2 *can be* uniquely *written as a product of primes? It doesn't. Convince yourself of this fact. Hint:* $(k+1)$ *can indeed be written as* $a \cdot b$ *and* $c \cdot d$ *for different* $(a, b), (c, d)$ *tuples. For example,* $36 = 4 \cdot 9 = 6 \cdot 6$.

3. **The Change Problem.** In the country of Borduria, they have three types of coins: a cent, a szlapot, and a dinar. A szlapot is worth 3 cents and a dinar is worth 7 cents. You have an unending supply of szlapots and dinars; show that any amount ≥ 12 cents can be made with only szlapots and dinars.

   You may have heard of similar such puzzles. In Math terms, it is stating the following theorem.

   Theorem 2. Prove that any natural number $n \geq 12$ can be expressed as $3x + 7y$ for *non-negative integers* x and y.

   Remark: *This may remind you of the theorem about* gcd; *since* $\gcd(3, 7) = 1$, *then there do exist* integers u *and* v *such that* $3u + 7v = 1$. *Clearly then,* $3 \cdot (12u) + 7 \cdot (12v) = 12$, *and we are done. No. Because* u *and* v *can be* negative, *and this is asking for non-negative integer linear combinations. Indeed, the number* 11 *cannot be written as* $3x+7y$ *for non-negative integers* x, y. *Please check this.*

   Proof. Let $P(n)$ be the predicate taking the value true if there exist non-negative integers (x, y) such that $n = 3x + 7y$. We need to prove $\forall n \geq 12, n \in \mathbb{N} : P(n)$.

   Base Case: Again, the base case here is $P(12)$, and indeed, $12 = 3 \cdot 4 + 7 \cdot 0$, and thus $P(12)$ is true. With hindsight, we know that just checking this will not suffice. So we go ahead and check $P(13)$ and $P(14)$ as well. Indeed, $13 = 3 \times 2 + 7 \times 1$, and $14 = 3 \times 0 + 7 \times 2$.

   Inductive Case: Since we have established $P(12), P(13), P(14)$ we need to establish $P(k)$ for $k > 14$. Fix a $k \geq 14$. The Induction Hypothesis is that $P(12), P(13), \ldots, P(k)$ are true. We now need to prove $P(k+1)$. That is, we need to find a way to write $(k+1)$ as $3x+4y$ for some non-negative integers (x, y).

   To see this, consider the number $m := (k+1) - 3$. Since $k \geq 14$, we see $m \geq 12$. Also, $m < (k+1)$, and therefore, $P(m)$ is true. That is, there exists non-negative integers (x', y') such that $m = 3x' + 4y'$. But $(k+1) = m + 3$, and therefore, $(k+1) = 3(x'+1) + 4y'$. Since $x' \geq 0$, $x'+1 \geq 0$ as well. Therefore, $(k+1)$ is expressed as $3x+4y$ with non-negative integers $x = x'+1$ and $y = y'$. Thus, $P(k+1)$ is proved, and by induction, $P(n)$ is proved for all $n \geq 12$. $\square$

   Remark: *In fact, the above proof also shows that any number* $n \geq 12$ *can be written as* $3x + 7y$ *where* x *and* y *are non-negative integers* and $y \leq 2$. *Do you see it? Make sure you see it.*

Remark: *There is a generalization of this problem which is called the* **Frobenius problem**. *It asks, given n non-negative integers $a_1, a_2, \ldots, a_n$ such that $\gcd(a_1, a_2, \ldots, a_n) = 1$ (that is, there is no number > 1 which divides all of the a_i's), find the* largest *number which* cannot *be expressed as $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots a_n \cdot x_n$ for non-negative integers $x_1, \ldots, x_n$. Note that the above theorem shows that when $a_1 = 3$ and $a_2 = 7$, the largest number is 11. So the answer to the Frobenius problem for $(3,7)$ is 11.*

Can you show that for any $(a_1, \ldots, a_n)$, there is some finite *number $F(a_1, \ldots, a_n)$ which is the answer to the above question? Or can it be infinity, that is, there is some $(a_1, \ldots, a_n)$ such that no matter what N you choose, there is a number $M > N$ such that M cannot be expressed as a non-negative integer linear combination of the a_i's?*

4. **Recurrences.**

In the analysis of algorithms (which is covered in depth in CS31), one often meets *recurrences* while trying to figure out running times of recursive algorithms. Perhaps, one meets a beast such as below.

Theorem 3. Consider the following recurrence: $t_1 = 1, t_2 = 3$, and $t_n = t_{\lceil n/2 \rceil} + t_{\lfloor n/2 \rfloor} + 1$ for all $n \geq 3$. Prove that

$$\forall n \in \mathbb{N} : \quad t_n \leq 2n$$

Let us first start with a failed attempt.

"Proof:" Let $P(n)$ be the predicate taking the value true if $t_n \leq 2n$ for that particular n. We wish to show $\forall n \in \mathbb{N} : P(n)$. We proceed by (strong) induction.

Base Case: This corresponds to the "base case" of the recurrence. $P(1)$ is true because $t_1 = 1 \leq 2 \cdot 1$, and $P(2)$ is true since $t_2 = 3 \leq 2 \cdot 2$. Thus both $P(1)$ and $P(2)$ are true; good.

Inductive Case: Fix a natural number $k \geq 2$. The Induction Hypothesis is that $P(1), \ldots, P(k)$ are true. That is, we have

$$t_a \leq 2a, \quad \text{for all } 1 \leq a \leq k. \tag{1}$$

We wish to prove $P(k+1)$. That is, we wish to establish $t_{k+1} \leq 2(k+1)$.

For brevity, we let $m := k+1$; so we wish to show $t_m \leq 2m$. Since $m \geq 3$, we know that

$$t_m = t_{\lceil m/2 \rceil} + t_{\lfloor m/2 \rfloor} + 1$$

Also since $m \geq 3$, both $\lfloor m/2 \rfloor$ and $\lceil m/2 \rceil < m$. Thus, by the Induction Hypothesis, both $P(\lfloor m/2 \rfloor)$ and $P(\lceil m/2 \rceil)$ are true. That is,

$$t_{\lceil m/2 \rceil} \leq 2\lceil m/2 \rceil, \quad \text{and} \quad t_{\lfloor m/2 \rfloor} \leq 2\lfloor m/2 \rfloor - 1$$

Putting these together, we get

$$t_m \leq 2\lceil m/2 \rceil + 2\lfloor m/2 \rfloor + 1 = 2\left(\lfloor m/2 \rfloor + \lceil m/2 \rceil\right) + 1 = 2m + 1 \tag{2}$$

Oh o! We wanted to show $t_m \leq 2m$, but what the above gives is off by 1. Yikes! ☹

This is an opportunity to tell of one of the coolest facts about proofs by induction:

It is often easier to prove something stronger.

Indeed, we will prove the following theorem.

Theorem 4. Consider the following recurrence: $t_1 = 1, t_2 = 3$, and $t_n = t_{\lceil n/2 \rceil} + t_{\lfloor n/2 \rfloor} + 1$ for all $n \geq 3$. Prove that

$$\forall n \in \mathbb{N} : \quad t_n = 2n - 1$$

Before proceeding, note that Theorem 4 implies Theorem 3. Indeed, if $t_n = 2n - 1$, then clearly $t_n \leq 2n$. Intuitively, it seems that proving something stronger, something more restrictive, should only be harder. But the following will show that your intuition is wrong. And yes, it is mind-blowing!

Proof. Let $P(n)$ be the predicate taking the value true if $t_n = 2n - 1$ for that particular n, and false otherwise. We will prove $\forall n \in \mathbb{N} : P(n)$ by strong induction.

Base Case: This corresponds to the "base case" of the recurrence. $P(1)$ is true because $t_1 = 1 = 2 \cdot 1 - 1$, and $P(2)$ is true since $t_2 = 3 = 2 \cdot 2 - 1$.

Inductive Case: Fix a natural number $k \geq 2$. The Induction Hypothesis is that $P(1), \ldots, P(k)$ are true. That is, we have

$$t_a = 2a - 1, \quad \text{for all } 1 \leq a \leq k. \tag{3}$$

We wish to prove $P(k+1)$. That is, we wish to establish $t_{k+1} = 2(k+1) - 1$.

For brevity, we let $m := k + 1$. Since $m \geq 3$, we know that

$$t_m = t_{\lceil m/2 \rceil} + t_{\lfloor m/2 \rfloor} + 1$$

Also since $m \geq 3$, both $\lfloor m/2 \rfloor$ and $\lceil m/2 \rceil < m$. Thus, by the Induction Hypothesis, both $P(\lfloor m/2 \rfloor)$ and $P(\lceil m/2 \rceil)$ are true. That is,

$$t_{\lceil m/2 \rceil} = 2\lceil m/2 \rceil - 1, \quad \text{and} \quad t_{\lfloor m/2 \rfloor} = 2\lfloor m/2 \rfloor - 1$$

Putting these together, we get $t_m = (2\lceil m/2 \rceil - 1) + (2\lfloor m/2 \rfloor - 1) + 1 = 2\left(\lfloor m/2 \rfloor + \lceil m/2 \rceil\right) - 1 = 2m - 1$. Thus, we have established $P(k+1)$ (rememeber, m was just a shorthand for $k+1$), and thus by induction we have the theorem. $\square$

Why could we prove something stronger so much more easily? The reason lies that the *induction hypothesis* was stronger too. Earlier, we wanted to prove $t_{k+1} \leq 2(k+1)$, but we could only assume (1), that is, $t_a \leq 2a$ for all $1 \leq a \leq k$. But in the second proof (the only correct proof), we could assume (3), that is, $t_a = 2a - 1$ for all $1 \leq a \leq k$. This is much stronger, and we could use this ammunition. But *note*: you have to prove something *stronger* too. It is *no longer* enough to prove $t_{k+1} \leq 2(k+1)$; you need to show that $t_{k+1} = 2(k+1) - 1$. (If you ask for more, you must deliver more).

The idea above is called *the method of strengthening the induction hypothesis.*

5. Another example of where strengthening helps. In class on Monday, we struggled to prove the following by induction.

Theorem 5. For any natural number n, prove that $\left(1+\frac{1}{n}\right)^n \geq 2$.

Instead consider the following much more more general theorem.

Theorem 6. Fix any real number $x \geq -1$. Prove that $\forall n \in \mathbb{N}$, we have $(1+x)^n \geq 1+nx$.

Do you see why Theorem 6 implies Theorem 5? For a given n, choose the real number $x := 1/n$. Since n is natural, we get $x > 0$ (and so, clearly ≥ -1). Substituting in Theorem 6 we get $(1+1/n)^n \geq 1 + n \cdot (1/n) = 2$.

How do we prove Theorem 6? I claim this is easy, and you should just stop what you are doing and prove this now. ✍

Exercise: *Prove Theorem 6 by induction on n.*