CS/Math 240: Introduction to Discrete Mathematics 2/10/2011

Lecture 7 : Strong Induction

Instructor: Dieter van Melkebeek Scribe: Dalibor Zelený

DRAFT

Last time we started discussing induction, a proof technique that is very important to computer scientists. For example, in computer science induction is the standard way for arguing program correctness, which is a topic we will discuss next week. Today we discuss a modification of induction called strong induction.

7.1 Induction Continued

Recall that in a proof by induction, we show that something holds for all natural numbers. To do so, we show it holds for zero and that if it holds for n, then it holds for $n+1$. We call the former the base case and the latter the inductive step.

In the last example in the previous lecture, we slightly deviated from the basic framework. In particular, we proved the following statement.

Theorem 7.1. *For all integers $n \geq 18$, a postage of n Cents can be realized using 4-Cent and 7-Cent stamps.*

Mathematically, this means

$$(\forall n \geq 18) \underbrace{(\exists a, b \in \mathbb{N}) n = 4a + 7b}_{P(n)}. \tag{7.1}$$

Statement (7.1) has the form of a statement that we can prove by induction. The predicate $P(n)$ depends on some natural number n, and we want to prove it for every n. The only way we deviate from previous examples of inductive proofs is that we are interested only in integers 18 and higher as opposed to all integers.

In the inductive proof, our base case was $P(18)$ instead of $P(0)$, and we proved the inductive step only for $n \geq 18$.

7.2 Strong Induction

We now discuss another modification of the inference rule for induction. In particular, we strengthen the induction hypothesis.

7.2.1 A Motivating Example

We prove that every integer has a prime factorization. The proof is by induction, but using the usual inductive hypothesis falls short of proving the inductive step.

Theorem 7.2. *Every integer $n \geq 2$ can be written as a product of primes.*

We make two remarks. First, recall that an integer p is *prime* if its only divisors are 1 and p itself. Second, note that the statement of Theorem 7.2 has the form $(\forall n)P(n)$, so induction seems to be a reasonable approach.

Proof. We give a proof by induction on n.

Consider the statement $P(n)$: n can be written as a product of primes. We prove $P(2)$ as the base case, and show for all $n \geq 2$ that $P(n)$ implies $P(n+1)$.

The base case is $P(2)$, and we can indeed write 2 as a product of primes because 2 is a prime.

Now we prove the induction step, i.e., $(\forall n \geq 2)P(n) \Rightarrow P(n+1)$.

Assume that n can be written as a product of primes. We argue by cases.

Case 1: $n+1$ is prime. In this case, there is nothing to prove.

Case 2: $n+1$ is not prime. This means that $n+1$ has a divisor k such that $1 < k < n+1$. Hence, we can write $n+1$ as $n+1 = k \cdot l$ where $k, l \in \mathbb{N}$ and $1 < k < n+1$. (This is what it means for a number to have a divisor; also note that this means $1 < l < n+1$.) So now we have $n+1$ written as a product of two smaller numbers.

If we can find prime factorizations of k and l, we can combine those two factorizations and get a prime factorization of $n+1$ as follows

$$\begin{aligned} k &= p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \\ l &= p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r} \\ n+1 = kl &= p_1^{e_1+f_1} p_2^{e_2+f_2} \cdots p_r^{e_r+f_r} \end{aligned}$$

Unfortunately, our induction hypothesis only tells us we can write n as a product of primes, and says nothing about k or l.

It turns out that we can assume as our induction hypothesis that *every* $m \leq n$ can be written as a product of primes. (We take this for granted in this proof, and argue the correctness of such an assumption afterwards.) Stated this way, the induction hypothesis implies that both k and l have a prime factorization, and we can combine their prime factorizations into a prime factorization of n like we wanted.

It follows by induction that every integer greater than 2 has a prime factorization. □

We conclude this section with some other facts one can prove about prime numbers. We state these without proof.

- There are infinitely many primes. You can prove this by contradiction.
- Prime factorizations are unique up to the ordering of the factors. That is, if we have two prime factorization of an integer n, then any prime p appears the same number of times in both of them.

We will post a supplemental handout for students who need more background on primes and prime factorizations sometime before the end of this week.

7.2.2 Inference Rule for Strong Induction

We now justify that it is valid to use a stronger induction hypothesis like the one we used in the proof of Theorem 7.2.

Let P be some predicate, and suppose we want to prove the statement $(\forall n \in \mathbb{N})P(n)$. This is the situation we were facing when proving Theorem 7.2.

Consider the predicate $Q(n)$: For all natural numbers $m \leq n$, $P(m)$ holds. In the case of Theorem 7.2, $Q(n)$ says that for all $m \leq n$, m can be written as a product of primes. This is exactly what we used as our stronger induction hypothesis.

Next, observe that $Q(n+1)$ is logically equivalent to $Q(n) \wedge P(n+1)$. Thus, assuming $Q(n)$ and showing that $P(n+1)$ holds as a consequence proves $Q(n+1)$. In our proof of Theorem 7.2, this corresponds to showing that if all integers between 2 and n have prime factorizations, then so does $n+1$, which actually proves that all integers between 2 and $n+1$ have prime factorizations.

Finally, since $Q(n)$ is more general than $P(n)$, $(\forall n)Q(n)$ implies $(\forall n)P(n)$. Thus, proving $(\forall n)Q(n)$ suffices to show that $(\forall n)P(n)$ holds. This is exactly what we did in the proof of Theorem 7.2.

As a side note, we mention that $(\forall n)Q(n)$ is in fact logically equivalent to $(\forall n)P(n)$.

We can also think of the predicate $Q(n)$ as $P(0) \wedge P(1) \wedge \cdots \wedge P(n)$, which we rewrite in more compact form as

$$Q(n) = \bigwedge_{k=0}^{n} P(k)$$

so as to avoid the lengthy notation that uses ellipsis $(\dots)$ and to remove any ambiguity such notation may cause.

The inductive step in strong induction corresponds to proving $P(0) \wedge P(1) \wedge \cdots \wedge P(n) \Rightarrow P(n+1)$, or, written more compactly, $\bigwedge_{k=0}^{n} P(k) \Rightarrow P(n+1)$.

Finally, we state the inference rule for strong induction.

$$\frac{\begin{array}{l} P(0) \\ (\forall n \in \mathbb{N}) \;\; \bigwedge_{k=0}^{n} P(k) \Rightarrow P(n+1) \end{array}}{(\forall n \in \mathbb{N}) \;\; P(n)} \tag{7.2}$$

Like we did with regular induction, we sometimes have a base case of $P(m)$ for some other m, which changes (7.2) to

$$\frac{\begin{array}{l} P(m) \\ (\forall n \in \mathbb{N}) \;\; n \geq m \Rightarrow (\bigwedge_{k=m}^{n} P(k) \Rightarrow P(n+1)) \end{array}}{(\forall n \in \mathbb{N}) \;\; P(n)}$$

We remark that we haven't actually done anything new here. Last lecture we proved a statement of the form $(\forall n)P(n)$ by strengthening $P(n)$ to $P'(n)$, proving $(\forall n)P'(n)$, and showing that $P'(n)$ implies $P(n)$. Deriving strong induction from regular induction is just another example of that procedure.

7.2.3 Another Example of Strong Induction: Unstacking Game

Consider the following game. Start with a pile of n boxes. In every step, take one pile that consists of more than one box and split it into two piles of one or more boxes each. The score for that step is the product of the sizes of the two new piles made in that step. The game keeps going until all piles are of size 1. The score for the game is the sum of the scores from the individual steps, and the goal of the player is to maximize the score.

Example 7.1: Let's start with one stack of 5 boxes, and take the following steps.

1. Break the stack into two stacks of 2 and 3 boxes, respectively. This gives us a score of $2 \cdot 3 = 6$.

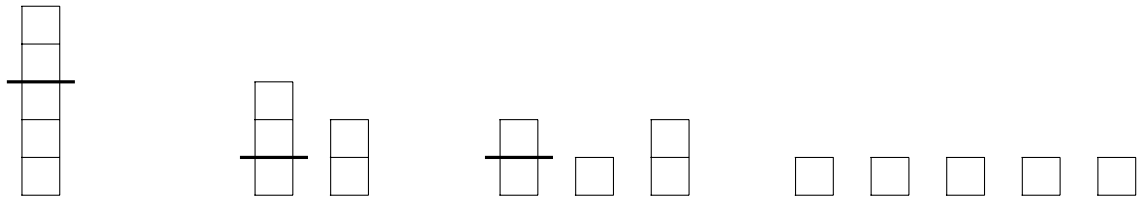
2. Break the stack of 3 boxes into a stack of 1 box and a stack of 2 boxes. This gives us a score of $1 \cdot 2 = 2$.

3. Take one of the stacks of 2 boxes and break it into two stacks of one box each. This has a score of $1 \cdot 1 = 1$.

4. Now take the other stack of 2 boxes and split it into two stacks of one box each. The score for this step is 1.

We show the state of the game at the beginning and after some of the steps in Figure 7.1.

After the four steps above, we are left with five stacks of one box each, so the game is over. Our total score is $6 + 2 + 1 + 1 = 10$. ⊠



(a) Initial state. (b) After step 1. (c) After step 2. (d) End of the game

Figure 7.1: One play of the unstacking game. We start with 5 boxes. The thick horizontal line in the graphic for each step indicates which stack of boxes is getting broken into two.

We want a strategy that maximizes the score at the end of the game. We explore possible moves and what scores they lead to on an example of a game that starts with 10 boxes. After trying different initial moves, we find that no matter what we do, we achieve a score of 45. Moreover, we saw in a previous example that starting with 5 boxes leads to a score of 10. Thus, we make the following conjecture.

Conjecture 7.3. *The score in the unstacking game depends only on the number of boxes we start with.*

The next step is to find what the score is if we start the game with one stack of n boxes. If we believe that the strategy doesn't matter, we should pick one for which the score is easy to calculate. One such strategy is to remove the top box from the only stack that has more than one box on it.

In the first step, we get $n-1$ points because we break the stack of n boxes into stacks of 1 box and $n-1$ boxes. In the second step, we get $n-2$ points because we break a stack of $n-1$ boxes into stacks of 1 box and $n-2$ boxes. This process continues, and in the last step we break a stack of 2 boxes into two one-box stacks for one last point. Thus, the final score is $(n-1)+(n-2)+\cdots+2+1$, which we write more compactly as

$$\sum_{i=1}^{n-1}(n-i). \tag{7.3}$$

One way to read equation (7.3) is "the sum over all i from 1 to $n-1$ of $n-i$."

We can add up the terms in the summation in the opposite order and rewrite (7.3) as

$$\sum_{i=1}^{n-1} i. \tag{7.4}$$

In programming terms, think of this modification as a change in code that traverses an array in the forward direction instead of traversing it in the backward direction.

We proved last time that $\sum_{i=1}^{r} i = \frac{r(r+1)}{2}$, so our total score (given by (7.4)) is $\frac{n(n-1)}{2}$ with this strategy.

Finally, we formulate our conjecture as a theorem and prove it using strong induction. A game with zero boxes is rather boring, so we choose our base case in the proof below to be a game with one box.

Theorem 7.4. *For all n, any strategy in the unstacking game starting with n boxes leads to a score of $\frac{n(n-1)}{2}$.*

Proof. We prove by strong induction that $(\forall n)P(n)$ where $P(n)$ is the statement "Every strategy for n boxes leads to a score of $n(n-1)/2$."

In the base case $P(1)$, we play a game with one box. That game is over right away, so the score is 0. Note that $0(0-1)/2 = 0$, so $P(1)$ is proved.

For the induction step, we prove $(\forall n \in \mathbb{N})\,(\bigwedge_{k=1}^{n} P(k)) \Rightarrow P(n+1)$.

Let $n \geq 1$ be an integer and suppose $(\bigwedge_{k=1}^{n} P(k))$, that is, suppose that for every integer k such that $1 \leq k \leq n$, every strategy for a game that starts with k boxes leads to a score of $k(k-1)/2$.

Now consider a game where we start with a stack of $n+1$ boxes. In the first step, we split our stack into stacks of k and $n+1-k$ boxes for some k that satisfies $1 \leq k \leq n$. The score for this step is $k(n+1-k)$. We can view the next steps as playing two separate games, one with a pile of k boxes and one with a pile of $n+1-k$ boxes.

The total score is then the sum of the following scores: (i) the score for the first step, (ii) the score from a game on k boxes, and (iii) the score from a game on $n+1-k$ boxes. This is

$$\underbrace{k(n+1-k)}_{(i)} + \underbrace{\frac{k(k-1)}{2}}_{(ii)} + \underbrace{\frac{(n+1-k)(n-k)}{2}}_{(iii)}, \tag{7.5}$$

where the last two terms in (7.5) come from the induction hypothesis. Now we find a simpler expression for (7.5).

$$\begin{aligned}
(7.5) &= \frac{2k(n+1-k) + k(k-1) + (n+1-k)(n-k}{2} \\
&= \frac{2kn + 2k - 2k^2 + k^2 - k + n^2 - kn + n - k - kn + k^2}{2} \\
&= \frac{n^2 + n}{2} \\
&= \frac{(n+1)n}{2}
\end{aligned}$$

Hence, the score we get in the game that starts with $n+1$ boxes is $(n+1)n/2$, which is what we wanted to show.

That finishes the proof. □