

Lecture 11: Proof by Induction.

8.1.1. Recursive definitions.....	1
8.4. Peano’s axioms and Proof by Induction.....	2
Homework 11.....	4
APPENDIX:.....	5
How to use Induction in a Proof.....	5
Introduction.....	5
Example 1.....	5
Example 2.....	7
Conclusion.....	8
Feedback.....	8

Read: PtMW, Chapter 8, Section 8.4 (192-198) and Section 8.5.7 (214-215).

Attention: Induction is a mind-bender, more than it seems at first!

8.1.1. Recursive definitions.

First let’s review recursive definitions from Section 8.1.1 of PtMW. There is in fact a close connection between being able to specify the membership of some set recursively and being able to use some version of the Principle of Mathematical Induction to prove that all members of the set have some property or other.

Consider the set M of all even-length mirror-image strings on $\{a,b\}$. An even-length mirror-image string is a string that can be divided into two halves, with the right half a mirror-image reversal of the left half (a “palindrome”). Examples: $abba$, $babbab$, $aaaa$, $bbabbabb$. Non-examples: $babb$, $aaab$, bab .

Recursive definition of M :

- (8-1)
1. $aa \in M \ \& \ bb \in M$
 2. $(\forall x)(x \in M \rightarrow (axa \in M \ \& \ bxb \in M))$
 3. *Nothing is in M except by virtue of rules 1 and 2.*

(Line 1 is called the *base* of the recursion, line 2 the *recursion step*, and line 3 is an obligatory *restriction* that is often omitted, but always understood to be included.)

The recursive step of a recursive definition looks a lot like a “circular definition”, as in the “definition” of *subset* in (8-2).

- (8-2) For any sets A and B , A is a subset of B iff every subset of A is a subset of B .

The “definition” in (8-2) is no good as a definition; it contains a vicious circle. But (8-1) is a perfectly good recursive definition. What makes the difference? The presence of the base, and the possibility of applying the recursive step repeatedly, one iteration at a time.

The derivation of a string $abaaba \in M$ can be presented in a form virtually identical to the form of a proof.

- | | | |
|-------|--|-----------------------------|
| (8-3) | 1. $aa \in M \ \& \ bb \in M$ | Ax. 1 |
| | 2. $(\forall x)(x \in M \rightarrow (axa \in M \ \& \ bxb \in M))$ | Ax. 2 |
| | 3. $aa \in M$ | 1, Simplification |
| | 4. $aa \in M \rightarrow (aaaa \in M \ \& \ baab \in M)$ | 2, Universal Instantiation |
| | 5. $aaaa \in M \ \& \ baab \in M$ | 3,4, Modus Ponens |
| | 6. $baab \in M$ | 5, Simplification |
| | 7. $baab \in M \rightarrow (abaaba \in M \ \& \ bbaabb \in M)$ | 2, Universal Instantiation. |
| | 8. $abaaba \in M \ \& \ bbaabb \in M$ | 6,7, Modus Ponens |

And we could keep going. Deriving longer strings just requires longer proofs with more of the same sorts of steps.

We can similarly give a recursive definition of the wffs of statement logic. (See pp 182-183.) If we want to have the possibility of arbitrarily many basic statements, $p, q, r, p', q', r', p'', q'',$ etc., then we have to start with a recursive definition of atomic statement, and then use that in giving a recursive definition of the set of all wffs.

8.4. Peano's axioms and Proof by Induction.

In this section we will look at an axiomatic approach to the natural numbers. "Peano's axioms" for the natural numbers, actually due to Dedekind, are one of the most well-known axiomatic systems in the history of mathematics. And they also give rise to the important *Principle of Mathematical Induction* and the related technique of *proof by induction*.

In the axiomatic approach to natural numbers, the aim is to set forth some essential properties of the natural numbers from which all their other properties are derivable as theorems, just as in Euclid's axiomatization of plane geometry.

We start with three primitive (undefined) notions: two primitive predicates and one primitive constant. (i) a 1-place predicate 'is a natural number', which we will symbolize by Nx ; (ii) a 2-place predicate 'is a (the) successor of': we write Sxy for ' x is successor of y '; (iii) the constant 0.

The axioms:

P1. $N0$ (0 is a natural number)

P2. $(\forall x)(Nx \rightarrow (\exists y)(Ny \ \& \ Sxy \ \& \ (\forall z)(Szx \rightarrow z = y)))$ (Every natural number has a unique successor.)

P3. $\sim(\exists x)(Nx \ \& \ S0x)$ (0 is not the successor of any number.)

P4. $(\forall x)(\forall y)(\forall z)(\forall w)((Nx \ \& \ Ny \ \& \ Sxz \ \& \ Swy \ \& \ z=w) \rightarrow x = y)$ (No two distinct natural numbers have the same successor.

P5. If Q is a property which has properties (i) and (ii) below,

(i) $Q0$ (zero has Q), and

(ii) $(\forall x)(\forall y)((Nx \ \& \ Qx \ \& \ Ny \ \& \ Syx) \rightarrow Qy)$ (if a natural number has Q then its successor has Q , i.e. Q is a ‘hereditary’ property)

then $(\forall x)(Nx \rightarrow Qx)$ (every natural number has Q)

The fifth Peano postulate is very important; it introduces the notion of mathematical induction. It is not and cannot be expressed in our familiar first-order predicate logic, because it involves quantification over a second-order property Q . Intuitively, it is an axiom that says that the natural numbers are subject to the “domino effect”: Whenever you find a property that holds of (“knocks down”) zero, and such that when it holds of (“knocks down”) any number it must hold of its successor, you can conclude that it holds of (“knocks down”) all numbers.

The first four axioms guarantee the existence of an infinite chain of numbers. The fifth one makes sure that there is no more than the one infinite chain guaranteed by the first four.

The *intended model*: 0, 1, 2, 3,

(Other models: you can find some in section 8.5.7. For instance: the set of all multiples of 5: 0, 5, 10, 15, In this case “natural number” is interpreted as “non-negative multiple of 5”, “0” is interpreted as 0, and “y is successor of x” is interpreted as “y = x+5”.)

A simpler form of P5, suppressing N (assuming that our domain of quantification is just the natural numbers) and writing $\text{Succ}(x)$ for the number which is successor of x (which is legitimate given that the first four axioms guarantee that the successor relation is actually a function):

For any predicate Q , if the two statements in 1 and 2 are both true of Q :

1. $Q0$

2. $(\forall x)(Qx \rightarrow Q(\text{Succ}(x)))$

then the following statement is also true of Q :

3. $(\forall x)Qx$

The axiom P5 is actually the principle of mathematical induction. P5 as an axiom states that the principle of mathematical induction is valid on the natural numbers. It provides a rule of inference that can be applied to statements about the natural numbers. Any proof that uses this rule of inference is called a *proof by induction* or an *inductive proof*.

The general form of a proof by induction:

First establish $Q(0)$.

Then establish (usually via conditional proof plus Universal Generalization) the truth of the second premise, i.e. the truth of the statement $(\forall x)(Q(x) \rightarrow Q(x+1))$.

Then you are entitled to conclude (“by Mathematical Induction”): $(\forall x)Q(x)$.

Where the hard work comes in: First, in figuring out what the relevant property Q should be, and second, in proving $(\forall x)(Q(x) \rightarrow Q(x+1))$.

Because the proof of $(\forall x)(Q(x) \rightarrow Q(x+1))$ usually requires U.G. (Universal Generalization), you have to be really sure that you are considering “an arbitrary number”, and proving that for *any number x at all*, if Q holds of x , then it must hold of $x + 1$. This takes getting used to.

Example: Prove for all n that $0 + 1 + \dots + (n-1) + n = \frac{n \cdot (n + 1)}{2}$ (This example is also done in the **appendix**, with additional discussion.)

Steps: First identify the property Q .

$$Q(k) \text{ is: } 0 + 1 + \dots + (k-1) + k = \frac{k \cdot (k + 1)}{2}$$

Then step 1: Prove $Q(0)$

Then step 2: Prove that for all k , $Q(k)$ implies $Q(k+1)$. Do it by conditional proof. So start by assuming that $Q(k)$ holds for some *arbitrary natural number k* and prove that Q must then hold of $k+1$. Then by the rule of Conditional Proof followed by U.G., you can conclude, as desired, that $(\forall k)(Q(k) \rightarrow Q(k+1))$.

THEN you can conclude, by Mathematical Induction, that

$$(\forall n) (0 + 1 + \dots + (n-1) + n = \frac{n \cdot (n + 1)}{2})$$

More examples in the text and in the homework and in the Appendix, from David Hofer’s website. It is entirely natural for this not to make sense at first. But try, and redo and/or do more exercises until you get it straight and it makes sense.

Homework 11

PtMW pp. 232-233, Exercises 4 and 5, optionally 3, optionally 6 (about the ‘proof’ that all horses are the same color.)

(You can find answers to 4, 5, and 6 on the 2001 and 2004 websites; in 2001 it was Homework 11; in 2004 it was Homework 10.)

APPENDIX:

<http://www.cs.uoregon.edu/~dhofer/induction.html> found October 18, 2004.

This is by David Hofer, a M.Sc. student in Computer and Information Science at the University of Oregon. For more about him, see <http://www.cs.uoregon.edu/~dhofer/index.html>.

How to use Induction in a Proof.

Introduction

If writing proofs is a craft, as some mathematicians believe, then induction is a useful tool for a proof-writer to possess. It can be used to demonstrate a fact about an infinite number of things, without having to write a proof which is infinitely long, or even more than a page in most cases. That's a powerful kind of abstraction. But it is not an easy one to understand. I was halfway through getting my master's degree before I realized exactly why induction is a valid thing to use. I also realized that every time I'd had induction explained to me, whether by a teacher or a book, the true motivation for it wasn't really provided. Most books describe induction as requiring a base case and an inductive step. Once you've proven those two cases, they say, you've completed the proof. But those two steps seemed to me like getting something for nothing. And I was uncertain about the inductive step. It seemed a little unreasonable to assume that the proof was correct up to some arbitrary value of n . However, as long as it is used properly, induction is a perfectly valid way of proving something. The trick is to know how to use it. In many crafts, it is not necessary to know how to build the tools you use, but in mathematics, if you understand how a tool is constructed, you can probably use it better. This document, then, is partly about how induction came to exist as a mathematical tool. It is also about how to use it, and contains several examples.

First, we will look at a simple problem which can be proved by induction, but we will try to prove it without using induction. Hopefully, this will give a good intuitive idea of how induction can be used.

Example 1

Prove that, in any full binary tree of height n , there are 2^n [i.e. 2^n] external nodes.

(A binary tree consists of a root and descendant nodes. Each node, including the root, has at most 2 children. An external node [terminal node] has no children, while an internal node has 1 or 2 children. An edge is the line that links a parent node to a child node. The height of the tree is the distance, in edges, from the root to the farthest external node from it. The depth of a node is the distance, in edges, from it to the root. In a full binary tree, every internal node up to a certain depth d has 2 children; any node at depth $d+1$ is an external node. For more details on binary trees, see the CIS 313 textbook Data Structures and Algorithms in Java by Goodrich and Tamassia or Introduction to Algorithms by Cormen, Leiserson, Rivest.)

The first thing to do for this proof, as with any proof, is to think about examples of the thing we're trying to prove. For a binary search tree that consists of just the root (which is a full tree), the height of the tree is 0, and the number of external nodes is $2^0 = 1$. Since the root is an external node in this case, we have confirmed that what we are trying to prove holds. Now

let's look at the next largest full binary tree, one with height 1. This contains the root node and its two children, each of which is an external node. The height of the tree is 1, and the number of external nodes is $2^1 = 2$, so we're fine.

For a full binary tree of height 2, the root has 2 children and 4 grandchildren. Each grandchild is an external node. Since the height of the tree is 2, we again verify that the number of external nodes is the same as $2^2 = 4$. For a full binary tree of height 3, the grandchildren of the root are now internal nodes, but each of their children is an external node. Since each grandchild has 2 children, and there are 4 grandchildren, there must be 8 external nodes. We again verify that $2^3 = 8$.

In the statement about a full binary tree of height 3, our analysis of the problem slipped a little. Instead of explicitly describing the entire tree, we described it from the root to the nodes of depth 2. We then said, "The nodes at depth 2 are internal and each has 2 children, so the number of nodes at depth 3 must number twice as many as the nodes at depth 2." That statement is an inference based on the fact that we know how many nodes are at one depth, and we know how each one relates to the nodes at the very next depth. For every node at the lower depth, there are two nodes at the next higher depth, since the nodes at the lower depth all have two children.

So, now we know that there are 8 nodes at depth 3. Additionally, we know that for any full binary tree of height greater than 3, there will still be 8 nodes at that depth. In particular, for a full binary tree of height 4, we can use those facts to infer, once more, that since the 8 nodes at depth 3 all have 2 children, there must be 16 nodes at depth 4. Once more, we verify that $2^4 = 16$.

Continuing on, from all the facts we've described above, we know that in a full binary tree of height 5, each of the 16 nodes at depth 4 must have 2 children, and so there are 32 nodes at depth 5. So there are 32 external nodes. Since $2^5 = 32$, our hypothesis continues to hold.

Hopefully by this point, the analysis is getting boring. If we continued to show how many external nodes there are for any arbitrary full binary tree, the proof would stretch off to infinity, covering trees of height 6, 7, 8, 9, and so on. But the pattern of how we move from one level of the tree to the next should be apparent. We have shown that in a full binary tree of height h , at most 5, there are 2^h external nodes. For the last 3 levels, we've shown this by assuming how many nodes there are at the previous level, which in turn was proved in the previous step, and then inferring how many nodes there are at the current level. This seems like a pretty solid way of proving this for each level. But considering the case where h equals, say, 97, it would take a lot of time to prove that the number of external nodes was 2^{97} , since we would have to prove that there are 2^{96} external nodes at level 96, which in turn means we have to prove that there are 2^{95} nodes at level 95, and so on down to level 5, which was our last level where this was definitely proven.

Here is where induction can help us. Induction is the mathematician's shorthand for saying, "If you grant me that what I am trying to prove is true at a certain level, then I can show that it is also true at the next level." But it is an abstraction over all the levels! We only need to

assume that we are considering one arbitrary level, whether it is a binary tree of height 6 or height 65,536, and that our hypothesis holds for the level right before it. In that case, we only have to show that our hypothesis holds for the current level. If it does, then it must hold for all levels, because we assumed only that we were proving it for any one arbitrary level.

The one other requirement for induction is that we establish that a base case is true. An acceptable base case for the above proof would be a full binary tree of height 0 (ie just the root). From that base case, we could get to the case where the height is 1, then 2, and so on. But if we had no base case, we couldn't move on, because there would be no case that we could assume was true, and base the rest of the inductive argument on.

Given the previous discussion, here is a proof that a full binary tree of height h has 2^h external nodes. Consider a full binary tree of height 0. It is clearly just the root node, which is an external node. $2^0 = 1$, so for $h = 0$, the number of external nodes, 1, is 2^h . So we have established our base case. Now assume that $h = n-1$ for some value of $n > 1$. Our inductive hypothesis is that the number of external nodes in a full binary tree of height $n-1$ is $2^{(n-1)}$. Consider a full binary tree of height n . We can obtain this tree from a full binary tree of height $n-1$ by adding 2 children to each of the smaller tree's nodes. But then the number of external nodes would be $2 \cdot 2^{(n-1)}$, by the inductive hypothesis, since there were $2^{(n-1)}$ nodes at level $n-1$, and each of those nodes has 2 children. But $2 \cdot 2^{(n-1)} = 2^n$, and so for any full binary tree of arbitrary height n , the tree has 2^n external nodes.

Example 2

Here is another example to show another use of induction. The previous example involved binary trees; this one is about a summation of natural numbers.

Prove by induction that for all $n \geq 1$, the sum $1 + 2 + 3 + \dots + n = (n \cdot (n+1))/2$.

This is the result discovered by the mathematician Carl Friedrich Gauss at age 7, when asked to sum the numbers from 1 to 100. It is normally proven by considering the pairs $(1, n)$, $(2, n-1)$, ..., $(n/2, (n/2)+1)$ if n is even. If n is odd, a similar strategy can be used but there will be a number in the middle of the sum which cannot be paired up, simply because there are an odd number of numbers in the sum. But that's just a detail. If n is even, then the sum of the numbers in each pair is $n+1$, and there are $n/2$ pairs. So the sum of all the numbers is $n/2 \cdot (n+1) = (n \cdot (n+1))/2$.

However, this result can also be proven by induction. Consider the case where $n = 1$. Obviously, the sum of all numbers between 1 and 1 is 1. To verify our hypothesis, $1 \cdot (1+1)/2 = 2/2 = 1$, and so our summation formula holds for $n = 1$.

Consider the case where $n = 2$:
 $1 + 2 = 3$, and $2 \cdot (2+1)/2 = 2 \cdot 3/2 = 3$.

Consider the case where $n = 3$:
 $1 + 2 + 3 = 6$, and $3 \cdot (3+1)/2 = 3 \cdot 4/2 = 6$.

Consider the case where $n = 4$:

At this point, we can see that this sum equals the sum when $n = 3$, plus 4. So $6 + 4 = 10$, and $4 \cdot (4+1)/2 = 20/2 = 10$.

When $n = 5$, the sum is the previous one plus 5, which is $10 + 5 = 15$. To verify the formula, $5 \cdot (5+1)/2 = 30/2 = 15$.

By this point, we should certainly have the intuition required for the inductive hypothesis, which is the following: Assume that for some value n , the summation of $1 + 2 + \dots + (n-1)$ is $((n-1)((n-1) + 1))/2 = ((n-1) \cdot n)/2$. We are just substituting $n-1$ into our hypothesized formula for summation, so this is our inductive hypothesis. We are allowed to assume this because n can have any value greater than 0, and we will show that if the formula holds for the sum from 1 to $n-1$, then the formula will also hold for the sum from 1 to n .

We have already proved, by example, the cases where n is any number from 1 to 5. Let's say that our base case is $n = 1$, which has been shown already. We will now show it for general n . Using our inductive hypothesis, we can assume that $1 + 2 + \dots + n-1$ is $((n-1)((n-1) + 1))/2 = ((n-1) \cdot n)/2$. Suppose we added n to this value. We have:

1. $((n-1) \cdot n)/2 + n =$
2. $((n-1) \cdot n)/2 + 2 \cdot n/2 =$
3. $((n-1) \cdot n + 2 \cdot n)/2 =$
4. $((n-1 + 2) \cdot n)/2 =$
5. $(n \cdot n)/2 =$
6. $(n \cdot (n+1))/2$.

Line 1 is just an extension of the inductive hypothesis. Lines 2 and 3 change n so it can be added to the main term. Line 4 is the really tricky part of the proof; in this line we factor n out of the terms $(n-1) \cdot n$ and $2 \cdot n$, which allows us to combine $n-1$ and 2 to get $n+1$ in line 5. Line 6 uses the commutativity of multiplication ($a \cdot b = b \cdot a$) to rewrite the equation into the form originally given.

Thus we have shown by induction that the sum of numbers from 1 to n is always $(n \cdot (n+1))/2$.

Conclusion

Induction is useful because an argument about an infinitely large number of cases can be squeezed into an argument about an arbitrary case out of the infinite number. But you don't get something for nothing from doing so; the inductive step is a very subtle one. Hopefully the examples in this document provide some insight into how to use induction properly.

Feedback.

The present maintainer of this page is dhofer@cs. Please send him any comments you may have. If you have any other proofs that you think could be explained well on this page, he would be interested to hear about them.