Foundations of Computer Science, Spring 2019

Induction Junction, or, tips on reading, understanding and doing proofs*

Induction is useful for proving assertions about natural numbers. The set of natural numbers, $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$. You will want to use it to show some statement/property, P, is true for the set of natural numbers.

Form: Prove statement P(n) is true for each integer n in the set of natural numbers with some restriction, e.g. for all $n >= n_0$.

Why it works: You can define natural numbers in a recursive way; In order to list the natural numbers, *start with 0* and repeatedly *add one*. So, you can prove P is true by a) *showing that 0* has property P and b) *whenever you add one* to a number that already has P, the resulting number also has the same property. Thus, like falling dominos, all natural numbers have this property P.

Variations: The initial starting point does not have to be 0 or even 1. A proof could start with, say, all even numbers, or all numbers > some arbitrary value. In cases such as these, you still have a starting point (i.e. Base Case) to consider. Also, instead of adding one, you could add negative one and accomplish the same task.

Procedure: There are ~~four~~ five general sections to resolve.

1. Rewrite what it is you are trying to prove and ensure the variables and conditions/restrictions are noted. Usually they are expressed in terms of n.
2. Prove that the Base Case is true, and the first domino falls.
3. Write the inductive hypothesis as an assumption: assume the k^{th} domino falls.
4. Prove the inductive case. Use the inductive hypothesis to show that domino $k+1$ also falls.
5. Then the property is proven true for the identified set of natural numbers.

Side notes: 1) For anything defined by recursion, the preferred proof technique is induction. This is because of the same idea that guides our proofs of transitivity, set equality, etc. – we simply need to follow the relevant definitions. So, when we prove something by induction, we are typically guided to do so by an underlying recursive definition. 2) Makinson recommends using k and $k+1$ in the proof, instead of the variable in the problem statement, n. This helps to separate sections and can reduce confusion when rereading a proof. 3) Optionally, and before writing a proof, you can make use of a work area to convince yourself that an assertion is true. 4) As we saw last week, we can utilize and maintain an equation where we update (only) one side of the equation (and comment the action this step takes!) Some proofs do not need to maintain LHS=RHS style statements.

We will review two example proofs.

(example 6.1.3 from Velleman) **Prove that $\forall n >= 5, 2^n > n^2$.**

Step 1: We want to show that for the set of natural numbers, all n that are greater than or equal to 5, the following inequality holds: $2^n > n^2$.

Step 2: Base Case (No need to start with 0 or 1 for this problem.) When n = 5, then

*D. Solow, *How to Read and Do Proofs*, Uniqueness Methods and Induction (John Wiley & Sons, 2005)
D. Velleman, *How To Prove It*, Mathematical Induction (Cambridge University Press, 1994, 2006)
D. Makinson, *Sets, Logic and Maths for Computing*, Recycling Outputs as Inputs: Induction & Recursion (Springer-Verlag, 2008, 2012)

$2^n = 32$ and $n^2 = 25$. And, $32 > 25$.

Step 3: Inductive Hypothesis: Let k be an arbitrary value such that k >= 5. Suppose that $2^k > k^2$

Step 4: Induction: We need to show that $2^{k+1} > (k+1)^2$

We have $2^{k+1} = 2*2^k$ // by arithmetic

$> 2*k^2$ // by inductive hypothesis

$= k^2 + k^2$ // by arithmetic

$>= k^2 + 5*k$ // by arithmetic since $k >= 5$.

$= k^2 + 2*k + 3*k$ // by arithmetic. Break it up this way for next step.

$> k^2 + 2*k + 1$ // by arithmetic since $k >= 5$.

$= (k+1)^2$ // by arithmetic

Step 5: We have shown that $2^{k+1} > (k+1)^2$ and we have proven the assertion.

Side notes: the above steps switched between equality statements and inequality statements when necessary. Moving from k^2 to k^2 >= 5*k may have required, as Thomas Edison might say, some inspiration and perspiration to find. The key here may be to factor $(k+1)^2$ first and use what we know to find a value greater than the result of $k^2 + 2*k + 1$. Making use of a work area could be helpful for proofs like this one.

For the next example we need a few definitions:

1. Prime number: A positive integer `n > 1` is a prime number iff the only positive integers that divide `n` are `1` and `n`.
2. Division: An integer n divides an integer m if m = k*n for some integer k and with n !=0. (our "divisible by" definition), i.e. m/n = k

(example 11.3 from Solow) **Prove that ∀n >= 2, n can be expressed as a finite product of prime numbers.**

For this example we do not have to maintain LHS = RHS format!

Step 1: We want to show that for the set of natural numbers, all n that are greater than or equal to 2, can be expressed as a product of prime numbers.

Step 2: Base Case (No need to start with 0 or 1 for this problem either.) When n = 2, then both 1 and 2 are prime numbers and 1*2 = 2. Indeed, 2 itself is prime.

Step 3: Inductive Hypothesis: Assume that the statement is true for all integers in between 2 and k. I other words for all j such that 2 <= j <= k, j can be expressed as a finite product of prime numbers.

Step 4: We need to show that for 2 <= j <= k+1, j can be expressed as a finite product of prime numbers.

Part a: if k+1 is a prime number, then the statement is true.

*D. Solow, *How to Read and Do Proofs*, Uniqueness Methods and Induction (John Wiley & Sons, 2005)
D. Velleman, *How To Prove It*, Mathematical Induction (Cambridge University Press, 1994, 2006)
D. Makinson, *Sets, Logic and Maths for Computing*, Recycling Outputs as Inputs: Induction & Recursion (Springer-Verlag, 2008, 2012)

Part b: if k+1 is not a prime number, then we can make use of the definition of division!

Even though k+1 is not a prime number, it has a divisor, say p, that is prime. So, p divides k+1 means k+1= p*j. Now j must be an integer such that 2<=j<=k. (Not k+1. Why?) This is our inductive hypothesis!

Step 5. So, j can be expressed as a finite product of primes. Since p is prime, that means k+1 can be expressed as a finite product of prime numbers.

Side notes: I had to make use of divisible by again ??!? Luckily, we did not have to consider 0. The Solow text didn't seem to show how we know that p must be prime in step 4. It doesn't matter because we can establish that both p and j must have the same property. That is 2<=p<=k and 2<=j<=k. This is because k+1 is not a prime number and both p and j have to be less than k+1.

---- ---- ----- ------ ------- -------- --------- ----------

We can now make the following statement: $\forall$students n $\in$ cmpu-145, these next proofs can be completed for homework. This assignment is due April 9. Please hand in this assignment using a separate set of paper.

1. Prove that: for a set with $n >= 1$ elements, there are 2^n subsets that can be created from it. (This has a familiar ring to it.)
2. Prove that: for $n >= 1$, the following is true: $1 + 2 + 22 + \ldots + 2n\text{-}1 = 2^n - 1$.

*D. Solow, *How to Read and Do Proofs*, Uniqueness Methods and Induction (John Wiley & Sons, 2005)
D. Velleman, *How To Prove It*, Mathematical Induction (Cambridge University Press, 1994, 2006)
D. Makinson, *Sets, Logic and Maths for Computing*, Recycling Outputs as Inputs: Induction & Recursion (Springer-Verlag, 2008, 2012)