Why Johny Can't Induct - copyright Dan Gusfield July 24, 2001

This is part of my rant on induction. It was written for undergraduate students in algorithms or discrete math classes in CS.

Two particular problems I will discuss show up in every class and I don't know how to cure these problems except to give examples of the errors and discuss them directly, even though my comments may seem overly harsh and critical. I don't mean to embarrass anyone, just to make clear serious errors that some people still have about induction and proofs.

First consider the following problem: Prove that $\sum_{i=1}^{n} i \times (i!) = (n+1)! - 1$.

Here is a correct proof:

Basis: When $n = 1$ the summation gives $1 \times 1! = 1$ which is what the right hand side, $2! - 1$ gives also, so the basis is proved.

I.H. Suppose the claim is true for n up to k.

I.S. Consider $n = k + 1$. The left hand side is $\sum_{i=1}^{k+1} i \times (i!)$ which equals $\sum_{i=1}^{k} i \times (i!) + (k+1)(k+1)!$. By applying the I.H. to the sum part gives $(k+1)! - 1 + (k+1)(k+1)!$. That expression simplifies to $(k+2)(k+1)! - 1 = (k+2)! - 1$ which is the form of the claim for $n = k + 1$, and so the claim is proved by induction.

What is wrong with the following "proof"? The basis and I.H. are the same as above. The I.S. is:

$\sum_{i=1}^{k+1} i \times (i!) = ((k+1)+1)! - 1 = (k+2)! - 1 = (k+2)(k+1)(k)(k-1)! - 1$, so the case holds for $k + 1$ and the claim follows by induction.

What is wrong is that it starts by just asserting the very thing that we are to prove; and then it does a (correct) manipulation of the expression, followed by the statement that the case holds. But this does nothing. You cannot just assert what you are required to prove.

Now lets consider the last problem (6) on the midterm: Prove that n lines on the plane create $(n^2 + n + 2)/2$ regions. No two lines are parallel and no three intersect at a point. Here is a correct inductive proof:

Basis: $n = 1$. A single line clearly cuts the plane into two regions. Also, $(1^2 + 1 + 2)/2 = 2$, so the claim is correct for $n = 1$. We will see in the I.S. that a basis of size one is sufficient.

I.H. Suppose the claim is true for n up to k.

I.S. We want to prove the claim true for $n = k+1$. Consider any *arbitrary* configuration of $k + 1$ lines on the plane where no two are parallel and no

three meet at a single point. Take any particular line, call it L. Removing L leaves k lines. By the I.H. those k lines divide the plane into $(k^2+k+2)/2$ regions. Now consider putting back line L exactly where it was before its removal. In fact, consider penciling it in from one end to the other (of course you can't write it that way, since it is infinite, but you can think of it that way). Just before writing an intersection of L with an existing line, L will be inside a region R formed by the k lines already on the plane. At the moment of that intersection, L will close off a new region, dividing R into two regions. This happens every time L intersects a line of the existing configuration. How many new regions are created in this way? Since no line is parallel to L, L will intersect each of the k lines already in the configuration, and since no three lines meet at a point, L will intersect each of those k lines separately. That implies that k new regions are created. But there is an additional one region created on the other side of the last line that L intersects. Hence exactly $k+1$ new regions will be created by adding back L. That means that the number of regions created after L is drawn is exactly $k+1+(k^2+k+2)/2 = (2k+2+k^2+k+2)/2 = ((k^2+2k+1)+k+1+2)/2 = ((k+1)^2+(k+1)+2)/2$. Since $((k+1)^2+(k+1)+2)/2$ fits the form of the claim for $n=k+1$, the induction proof is done.

The above proof is perhaps overly complete and people certainly got full credit for saying much less, but it does show all the reasoning. Now consider the following "proof" which demonstrates a serious misunderstanding. Can you find the flaw?

Basis: When $n=3$ there are $(3^2+3+2)/2 = 7$ regions.

I.H. For some number k there are $(k^2+k+2)/2$ regions.

I.S. We must show that $k+1$ lines divide the plane into $((k+1)^2+(k+1)+2)/2$ regions.

Now $((k+1)^2+(k+1)+2)/2 = (k^2+2k+1+k+1=2)/2 = (k^2+3k+2)/2 = (k^2+k+2+2(k+1))/2 = (k^2+k+2)/2+k+1$. But $(k^2+k+2)/2$ is the number of regions there are with only k lines, and $k+1$ is the next term in the summation, so we have proven the claim by induction.

An alternative last line is: But by the induction hypothesis $(k^2+k+2)/2$ is the number of regions there are with only k lines, so the inductive proof is done.

What is wrong with the above "proof"? The answer is that it is only formal manipulation without any real content from the claim. Nowhere does

it discuss lines in the plane. How can you prove a formula about lines in the plane without bringing in some reasoning about lines and planes etc? Induction is a "style of proof" that is used to prove claims about mathematical objects (in this case about regions formed by lines in the plane). The proof has to deal with those particular mathematical objects - that is the heart of the proof. And the basis must do that also. Even the basis above does not show that three lines divides the plane into seven regions.

Pure manipulation of formula can't prove anything by itself. To make this point clearer, consider the following claim: Any n circles of diameter one divide the plane into $(n^2+n+2)/2$ regions. Assume no two circles have the same center. We will "prove" this claim by induction.

Basis: For $n = 1$ the plane is divided into two regions, as specified by the claim.

I.H. For some number k there are $(k^2+k+2)/2$ regions.

I.S. We must show that $k+1$ circles divide the plane into $((k+1)^2+(k+1)+2)/2$ regions.

Now $((k+1)^2+(k+1)+2)/2 = (k^2+2k+1+k+1=2)/2 = (k^2+3k+2)/2 = (k^2+k+2+2(k+1))/2 = (k^2+k+2)/2+k+1$. But by the I.H. $(k^2+k+2)/2$ is the number of regions there are with only k circles, and $k+1$ is the next term in the summation, so the inductive proof is done.

Surely, this "proof" is as valid as the second one above about lines and regions – the manipulations in the I.H. and I.S. are the same. But, in fact n circles do *not* divide the plane into $(n^2+n+1)/2$ regions. A method that is valid should not "prove" things that are not true. That should show you that the above manipulations do not constitute a correct induction proof.

Another example:

Close pairs problem Consider the numbers 0 through 2^n-1 written in binary. We say that numbers A and B form a close pair if their binary representations differ in exactly one bit. For example, 100 and 110 form a close pair because they differ in the second bit only. Numbers 110 and 001 do not form a close pair. Prove by induction that among the numbers 0 through 2^n-1, the number of close pairs is exactly $n \times 2^{n-1}$ for any integer $n \geq 0$.

Here is a correct proof: First, note the set of integers from 0 through 2^n-1 is exactly the set of numbers that can be represented in binary by using at most n bits. And so proving the formula correct for numbers 0 through 2^n-1 is the same as proving it for all numbers represented by using

at most n bits.

Basis: Setting n = 1 in the proposed formula gives $1 \times 2^0 = 1$, so the basis for n=1 is shown, and the basis is shown for all numbers using 1 bit.

Induction Hypothesis: Suppose that the formula is correct for $n \leq k$ i.e., for all numbers represented by at most n bits.

Induction Step: Using the induction hypothesis, we prove that there are $(k+1)2^k$ close pairs from the set of all $k+1$ bit numbers. Consider bit $k+1$ in a close pair. Either that bit is the same in both numbers or it is different. We consider the first case first. If bit $k+1$ is the same then both are either 0 or both are 1. In both cases, the pair is close only because the bits k through 1 of the two numbers form a close pair. By the induction hypothesis there are $k2^{k-1}$ of these pairs. So there are $2k2^{k-1}$ close pairs of $k+1$ bit numbers where bit $k+1$ is the same in each of the two numbers.

Second case: If the $k+1$ bit of one number in a close pair is not the same as the $k+1$ bit of the other number, then bits k through 1 must be the same. There are 2^k k bit numbers, so 2^k close pairs of this type.

Adding these two cases gives that the total number of close pair in the set of k bit numbers is $k2^{k-1}$. This completes the induction step. So by the principle of mathematical induction, the formula is proved.

Comment 1: Notice that proof the basis and the proof of the induction step is based on the particulars of close pairs. It is not just a manipulation of a formula.

Comment 2: There is a direct proof of this.

Direct proof: There are 2^n n bit numbers. If we take any such number and change any of its n bits we create a close pair for it. Example 00101 can be turned into its close partner by changing exactly one of its 5 bits, say bit 2 creating 00111. This suggests that there are $n2^n$ close pairs. However, that number double counts each close pair, since for example 00101 would also be created starting from 00111. So the correct number is half the above, i.e. $n2^{n-1}$ as claimed.

What is wrong with the following:

Basis step: P(1) is true since $1 \times 2^{1-1} = 1$.

I.H.: Assume P(n) is true, and we must show that P(n+1) is true. We do this by showing that when we "add the next term" to the formula given by the induction hypothesis, we get the correct formula for the next case.

That is, we will show that $n2^{n-1} + (n+1) = (n+1)2^n$.

In detail

$$n2^{n-1}+(n+1) = n(2^{n-1}+1)+1 = 2n(2^{n-1}+1)+2 = n(2^{n+1-1}+2)+2 = n2^n+2^n = (n+1)(2^n).$$

Therefore the number of close pairs is exactly $n^2n - 1$ for any $n \geq 0$.

What is wrong is that it just "adds the next term" without giving any justification for doing that. The problem is not the lack of justification itself. The problem is that without dealing with the substance of the problem, there is no reason why that is the correct next term to add. It is somewhere between nonsense and magic. Moreover, as detailed below, I do not advise the "adding the next term" approach.

Another Example

Consider a convex n-gon. Then add a straight line between any two non-adjacent corners of the n-gon. Continue adding straight lines between non-adjacent corners with the rule that no two lines you draw ever cross. Continue doing this in any way you like (while not violating the crossing rule) until you can't put in any more lines. Now consider the resulting drawing as the floor plan of a funny looking house where each line defines a wall. (There are no doors in this house). Prove by induction that there must be exactly $n - 2$ rooms in this house.

Answer: Basis: for $n = 3$ the house is triangle with one room.

I.H. Suppose such a house with $n \leq k$ sides has exactly $n - 2$ rooms.

I.S. Consider a $k+1$ side house and let L be one of the lines added in the interior of the $k+1$-gon the house was built from. L separates the house into two houses one on each side of L. These two houses together contain all the rooms of the original house, and no room is in both. If we duplicate L and its endpoints, then we have a house of k_1 sides and another of k_2 sides, where $k_1 + k_2 = k + 1 + 2$ (the additional two is for the two copies of L). Each of k_1 and k_2 is less than or equal to k (why?) so the I.H. applies to each, so the two houses have $k_1 - 2 + k_2 - 2$ rooms in total, which is the number of rooms in the original $k + 1$ side house. But $k_1 + k_2 = k + 3$ so the original house has $k + 3 - 4 = k - 1 = k + 1 - 2$ rooms as claimed. So the I.S. is finished, and by the princ. of M.I. any n sided house has $n - 2$ rooms. QED.

What is wrong with the following proof of the inductive step?

> Adding one more vertex to a k-gon adds two sides and these create a triangle to the division already done for the k-gon. This

triangle can't be further subdivided, and so exactly one more room is added to the division. By the I.H. there were $k-2$ rooms before the added triangle, so now there are $k-1 = (k+1)-2$ which finishes the I.S.

The problem with this proof is that it is not established that every possible division of a $k+1$-gon is created by adding a triangle to a division of a k-gon. If that were established the proof would be OK, and I would have given full credit. But one cannot just ignore the issue because the above proof gives a way to go from an arbitrary division of a k-gon to a *particular* division of a $k+1$-gon, leaving open the possibility that some $k+1$-gon has been ignored. A better approach is what I have written above which goes from an *arbitrary* division of $k+1$-gon to a particular division of a k-gon.

A closer to full variant of the incomplete proof was also given:

> I.S.: Find an edge in the $k+1$-gon division that goes from a vertex x to a vertex y exactly two vertices away. That line makes a triangle x, y, z enclosing a vertex z. So in this division of the $k+1$-gon, z has no added lines touching it. Now delete z and the two exterior sides that touch it from the $k+1$ gon, creating a k-gon with $k-2$ room (by the IH). Hence the $k+1$-gon has $k-1$ rooms.

This again has a problem of not establishing that the line x, y exists, or equivalently that such a vertex z exists. To be complete you have to show why there is a vertex z which has no added lines from it – it is conceivable (although not true) that all vertices have added lines out of them. In the proof I gave, we don't have to deal with this issue, because L is *any* of the added lines. The above proof is close to my proof, but has assumed (without proof or even assertion) that a special kind of line L must be in the division.

Another Example

Consider the following Claim (*): All trees with n nodes have exactly n-1 edges (lines).

Very common near proof: Basis: clearly true for trees with 1 node and two nodes. Induction hypothesis: Suppose the claim is true for all trees with k nodes. Induction step: If we take a k node tree T and add a new node and a new edge to any node of T, then we clearly get a tree with one more node

and one more edge, i.e. a tree with n+1 nodes and n edges. Therefore the induction step is proven, and with it the claim.

This is an (incorrect) example of forward looking induction step.

Before explaining what's wrong with the above "proof" I will present what I claim is a more acceptable proof.

Basis and induction hypothesis the same as above. Induction step: Let T be an arbitrary k+1 node tree. By definition, a tree has a leaf node, call it v. If we delete v and the edge it is attached to, we have a tree T' with k nodes. Therefore, by the induction hypothesis, T' has k-1 edges. Clearly T has one more node and one more edge than T' and so T has k+1 nodes and k edges. Therefore we have proven the above claim.

This is an example of backward looking proof of the induction step: You want to prove something about k+1 node trees so you look back to trees with fewer nodes.

The problem with the first "proof" is that in the induction step an arbitrary tree with k nodes is selected, and from that one a *particular* tree with k+1 nodes and k edges is generated. But we want to know that any arbitrary tree with k+1 nodes has k edges. The above "proof" isn't a proof unless you make the case that any arbitrary k+1 node tree can be generated by adding a node and edge to some k node tree. Well in fact they can all be generated in this way, but how do we know and prove it? One proof is by taking an arbitrary tree T with k+1 nodes, realizing it has a leaf, deleting the leaf and the edge its attached to, revealing a particular tree T' with k nodes. You then know that T can be generated from the particular tree T', by adding a new node and a new edge. Now all this work to make the proof correct is, in effect, doing the proof by the second method.

The key thing is that if you try to do an induction step in the forward direction you must make sure (prove) that your method of generation really generates all the objects of interest. In the above proof it does, but it has to be proven. Generally, the backward method is far cleaner, less prone to allowing mistakes, and corresponds more closely to recursive thinking than does the forward approach.

The take-home message

Now we abstract. We want to prove a claim about a set of objects; in our case the set is the set of all trees. We can partition the set into different subsets, so that the subsets can be put in some order. In our example, each

subset consists of all trees with the same number of nodes, and these integer numbers give an ordering to the subsets. The basis is a proof that the claim is true for all elements in the subsets at the beginning of the order (how many subsets you need to prove the basis for depends on what the inductive step needs). The inductive hypothesis is that the claim is true for all elements in subsets up to a arbitrary point in the ordering. Then you must prove that given the inductive hypothesis and basis, the claim is true for all elements in the next subset in the ordering. Now the easy mistake you can make in going forward is that you generate elements of the next subset, but you don't generate them all, or you don't prove that you generate them all. The backwards approach makes this a hard mistake to make. In the backward method you take an arbitrary element in the k'th subset, and make a change to it so that the resulting element is in the k-1'st subset or below.

Now lets go back to high school and criticize the way you first learned to do induction.

Define T(n) = the sum of the integers from 1 to n. Suppose we want to prove T(n) = n(n+1)/2. That is, we are trying to prove something about the infinite set T(1), T(2), T(3), T(4),..... . Clearly T(k) = T(k-1) + k. In high school you learned to do the induction step *forwards* by adding k to T(k-1) to generate T(k). (You might even have been shown a choo-choo train moving along the track generating successive T(k)'s).

In contrast, in this class our approach to proving the Induction Step is recursive, therefore backwards. We say T(k) can be broken down to T(k-1) plus k. Now you should quibble here a little. In this example, the difference in the two approaches is mostly pedantic. Adding k to T(k-1) clearly does generate T(k); no argument is needed and the forwards method is o.k. The problem is that when you do inductive proofs involving more complex objects, such as trees, graphs, programs etc. the generation question can get difficult. A backward looking proof of the induction step simply avoids this problem.

Another Example

True or false: Some leaf of any n edge tree is at level n.

True of course. I took Discrete Math at UCD and I can prove it by induction as follows.

Basis: Clearly true for trees with zero or one edge.

Induction Hypothesis: Suppose the claim is true for trees with k edges, i.e. in every tree with k edges, some leaf is at level k. Induction step: Let T

be an arbitrary tree with k nodes, hence with some leaf v at level k. Attach a new node, v', and a new edge to v, creating a tree T' with k+1 edges. Clearly, v' is one level deeper than v, hence is at level k+1, and the claim is proved by induction.

This "proof" is as right as the first "proof" for (*). It generates a set of trees for which the claim is true. But is it a proof that the claim is true for all trees? No it is not a proof! And the fact that (*) is true does not make the "proof" of (*) any more of a proof than this one is.

Yet Another Example

Problem Suppose you write n 0's and n 1's around a circle in some arbitrary order. It is known that no matter how you place the 0's and 1's, there is always a starting point on the circle so that a clockwise walk on the circle will encounter no more 0's than 1's at any point on the walk.

a) Give a proof of this fact by induction.

Generally students have problems with this because they try the "next case add-on approach", but they don't know what to add on and where. They realize it is not helpful to just add in one more 0 and one more 1 arbitrarily, and they sense that it is not completely kosher to specify a good place to put them. So they feel something is wrong, but they don't know what to do.

b) We want an $O(n)$-time algorithm to find one such starting point. Justify the correctness and the worst-case running time of the following method:

Pick a point arbitrarily on the circle. Walk clockwise keeping a running score of the number of 0's seen minus the number of 1's seen. That is, let Z denote the running score. Start the value of Z at 0 at the start of the walk. At each step, if a 0 is seen, increment Z, and if a 1 is seen, decrement Z. As you walk, let M denote the place in the walk where the largest value of Z is encountered, and let MZ denote that value. After the walk returns to its starting point, a good start can be selected as follows: Start a clockwise walk from the number in position M+1, i.e, one position after the position denoted by M.

Problem: Prove that this method is linear time (trivial) and is correct.

Another idea for an algorithm: walk counterclockwise keeping track of where the minimum value of Z is. Then a good starting position for a clockwise walk is at that minimum Z point. Prove this. How is this related to the previous solution?

Answers: Induction Problem: Clearly true for one one 0 and one 1. Now Assume true for some n. Now look at an arbitrary circle with $n+1$ 0's and 1's. Look clockwise for a 1,0 combination which must exist somewhere. When you find one, remove it, find a clockwise good starting point (which exists by the induction hypothesis), and then reinsert the 1,0. Then the old starting point will work — at the point where this pair is encountered, the number of 1's is greater or equal to the number of 0's, then one more 1 is added, and then is subtracted because of the 0, hence after those two numbers, the total is as it was in the previous traversal.

Proof that the first algorithm works. Let A be the arbitrary starting point of the walk used to find point M. We need to prove that point M+1 is a good starting point. Suppose that walking from point M+1 towards A, there is point B before A is reached where $k > 0$ more 0's are seen than 1's. But then the walk from A would have a running count of $MZ + k > MZ$ at B contradicting the choice of point M. So the walk from M+1 to the point just before A is fine. Moreover, there must be exactly MZ more 1's in that interval than there are 0's, since the interval from A to MZ has MZ more 0's than ones, and the total number of 0's and 1's is the same around the circle. Now at no point in the interval from A to M does the number of 0's exceed the number of 1's by more than MZ. Hence the walk starting from point M+1 is good in the that interval as well.

A good induction problem for a homework

Here is another summation type induction problem, but a result that I found interesting:

$$\sum_{i=2}^{i=n} \frac{1}{i(i-1)} = 1 - \frac{1}{n}$$

This also has a simple direct proof not using induction.