Discrete Mathematics
Inductive proofs

Saad Mneimneh

1 A weird proof

Contemplate the following:

$$\begin{array}{rcl} 1 & = & 1 \\ 1+3 & = & 4 \\ 1+3+5 & = & 9 \\ 1+3+5+7 & = & 16 \\ 1+3+5+7+9 & = & 25 \\ & \vdots & \end{array}$$

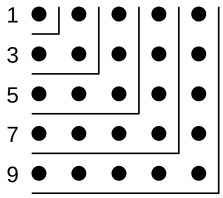
It looks like the sum of the first n odd integers is n^2. Is it true? Certainly we cannot draw that conclusion from just the few above examples. But let us attempt to prove it. The n^{th} odd number is $2n-1$, so our sum is the following:

$$\sum_{i=1}^{n}(2i-1) = 1+3+\ldots+(2n-1) = [1+3+\ldots+(2n-3)]+(2n-1)$$

But if the sum of the first n odd integers is n^2, then the sum of the first odd $n-1$ integers must be $(n-1)^2$. Therefore, our sum becomes

$$(n-1)^2+(2n-1) = n^2-2n+1+2n-1 = n^2$$

But is that legitimate? It seems that in our proof we used the very same fact that we are trying to prove! Or did we? In fact we did not. We used the fact for a smaller number ($n-1$ instead of n). Essentially, what we have established is the following: if the sum of the first $n-1$ integers is $(n-1)^2$, then the sum of the first n integers is n^2. And this works for any n. All we need now is a base case for some value of n, say n_0. But we have a base case because we enumerated few cases above. This technique is known as proof by induction. It is very simple, and least insightful. In deed, we did not gain any intuition why the sum of the first n odd integers is n^2 although we proved it. Here's a diagram that explains it.



The number of dots in a given layer is exactly two plus the number of dots in the previous layer. Starting with one dot in the first layer, each layer has an odd number of dots. Obviously, we always end up with a square after any number of layers. While this may offer a better intuition, induction remains an important tool for proving a formula that has only been guessed at by observation.

Here's another example that we have seen before. Let's prove that the sum of the first n integers is $n(n+1)/2$.

$$1 + 2 + \ldots + n = [1 + 2 + \ldots + (n-1)] + n = \frac{(n-1)n}{2} + n = \frac{n(n+1)}{2}$$

Again, the proof is only valid when a base case exists, which can be explicitly verified, e.g. for $n = 1$. Observe that no intuition is gained here (but we know by now why this holds).

2 Proof by induction

Assume that we want to prove a property of the integers $P(n)$. A proof by induction proceeds as follows:

- (base case) show that $P(1), \ldots, P(n_0)$ are true for some $n = n_0$
- (inductive step) show that $[P(1) \wedge \ldots \wedge P(n-1)] \Rightarrow P(n)$ for all $n > n_0$

In the two examples that we have seen so far, we used $P(n-1) \Rightarrow P(n)$ for the inductive step. But in general, we have all the knowledge gained up to $n-1$ at our disposal. So what is a proof by induction in English terms? First verify that your property holds for some base cases. Then given that your property holds up to $n-1$, you show that it must also hold for n. By the transitive property of implication, you have proved your property holds for all n.

$$\begin{gathered} P(1) \wedge \ldots \wedge P(n_0) \text{ is true} \\ [P(1) \wedge \ldots \wedge P(n_0)] \Rightarrow P(n_0+1) \\ P(n_0+1) \text{ is true} \\ [P(1) \wedge \ldots \wedge P(n_0+1)] \Rightarrow P(n_0+2) \\ P(n_0+2) \text{ is true} \\ \vdots \end{gathered}$$

That's pretty much it! The rest of this note covers examples of proofs by induction.

3 Some false proofs

Before we actually embark on a series of proofs by induction, let us make sure we have a good understanding of the mechanism. I will first prove by induction that the sum of the first n integers is

$$\frac{n^2+n+\sqrt{\pi}}{2}$$

Well, this is obviously true because

$$1+2+\ldots+n = [1+2+\ldots+(n-1)]+n = \frac{(n-1)^2+(n-1)+\sqrt{\pi}}{2}+n$$

$$= \frac{n^2+n+\sqrt{\pi}}{2}$$

What is wrong? There is no base case.

I will now prove by induction that any integer greater than or equal to 18 can be expressed in the form $4x+7y$ where both $x, y \geq 0$ are integers. It is certainly true for 18 when $x=1$ and $y=2$. So that will be my base case. Now assume that the property holds up to some number $n-1$, i.e. that $n-1$ can be expressed as $4x+7y$ where $x, y \geq 0$ are integers. I will show that the property remains true for n. Observe that $4(2)+7(-1)=1$. So

$$n = (n-1)+1 = 4x+7y+[4(2)+7(-1)] = 4(x+2)+7(y-1)$$

What is wrong? $y-1$ may be negative (if $y=0$).

Finally, I will prove by induction that any n lines, no two of which are parallel, pass through a single point. I will start with few base cases:

$n=0$: the statement is vacuously true
$n=1$: there is only one line, so trivially they all pass through a single point
$n=2$: the intersection of two lines is a single point

Now assume that this property holds up to $n-1$. I will show that it remains true for n. Consider n lines $l_1, l_2, \ldots, l_n$. The first $n-1$ lines $l_1, l_2, \ldots, l_{n-1}$ must pass through a single point, and that point must be the intersection of l_1 and l_2, say point p. Now consider the following $n-1$ lines: $l_1, l_2, \ldots, l_{n-2}, l_n$. They must also pass through a single point, and that point must be the intersection of l_1 and l_2, the same point p. Therefore, all n lines pass through p. What is wrong? Our n_0 is 2. The inductive step does not work for all $n > n_0$. It works for all $n > 3$. Can you see why (you need 4 lines to make it work)?

This example also sheds some light on the question of how many base cases are required in an inductive proof. In general, if your inductive step works for all $n > n_0$ for some n_0, then your base cases must cover up to n_0 (inclusive).

4 Example 1

Prove that the sum of the squares of the first n integers is $n(n+1)(2n+1)/6$, i.e.

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

When $n = 1$, this is $1(2)(3)/6 = 1$. This will serve as our base case. Now, for every $n > 1$, assume that the property holds up to $n - 1$ and show that it remains true for n.

$$1 + 2^2 + \ldots + n^2 = [1 + 2^2 + \ldots (n-1)^2] + n^2$$

$$= \frac{(n-1)n[2(n-1)+1]}{6} + n^2 = \frac{n(n+1)(2n+1)}{6}$$

To appreciate the power of induction, I will prove this by simply relying on our first two results, namely

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

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

The proof will require manipulations of sums.

$$\sum_{i=1}^{n} i^2 = \sum_{i=1}^{n}\sum_{j=1}^{i} (2j-1) = \sum_{i=1}^{n} [(n-i+1)(2i-1)]$$

The last equality holds because each term of the form $2i - 1$ appears exactly $n - i + 1$ times in the double sum. For instance, 1 appears n times, 3 appears $n-1$ times, 5 appears $n-2$ times, etc... Now we break the sum into its different parts:

$$\sum_{i=1}^{n} i^2 = \sum_{i=1}^{n} [(n-i+1)(2i-1)] = \sum_{i=1}^{n} 2ni - \sum_{i=1}^{n} n - \sum_{i=1}^{n} 2i^2 + \sum_{i=1}^{n} i + \sum_{i=1}^{n} 2i - \sum_{i=1}^{n} 1$$

Now every term that does not depend on i can be taken outside the sum to give:

$$\sum_{i=1}^{n} i^2 = 2n\sum_{i=1}^{n} i - n\sum_{i=1}^{n} 1 - 2\sum_{i=1}^{n} i^2 + \sum_{i=1}^{n} i + 2\sum_{i=1}^{n} i - \sum_{i=1}^{n} 1$$

We can now isolate the term $\sum i^2$ and combine similar terms,

$$3\sum_{i=1}^{n} i^2 = (2n+3)\sum_{i=1}^{n} i - (n+1)\sum_{i=1}^{n} 1$$

$$3\sum_{i=1}^{n} i^2 = (2n+3)\frac{n(n+1)}{2} - (n+1)n$$

$$\sum_{i=1}^{n} i^2 = \frac{(2n+3)n(n+1) - 2(n+1)n}{6} = \frac{(2n+1)n(n+1)}{6}$$

5 Example 2

Prove that if $a \neq 1$, then $\sum_{i=0}^{n} a^i = 1 + a + a^2 + \ldots + a^n = (1 - a^{n+1})/(1-a)$.

For $n = 0$, the above sum is 1, which is equal to $(1 - a^{0+1})/(1-a)$. Now, for every $n > 0$, assume the property holds up to $n - 1$ and show that it remains true for n.

$$1+a+a^2+\ldots+a^n = (1+a+a^2+\ldots+a^{n-1})+a^n = \frac{1-a^n}{1-a}+a^n = \frac{1-a^n+a^n-a^{n+1}}{1-a}$$

Again, to appreciate the power of induction, an alternative proof would have required a genuine observation that multiplying the sum by a corresponds to a shift (as opposed to a simple verification):

$$a\sum_{i=0}^{n} a^i = \sum_{i=0}^{n} a^{i+1} = \sum_{i=1}^{n+1} a^i = \sum_{i=0}^{n} a^i - 1 + a^{n+1}$$

$$(1-a)\sum_{i=0}^{n} a^i = 1 - a^{n+1}$$

6 Example 3

Prove that $n^3 - n$ is a multiple of 3 for all $n \geq 0$.

When $n = 0$, this is $0^3 - 0 = 0$, a multiple of 3. This will serve as our base case. Now, for every $n > 0$, assume that the property holds up to $n - 1$ and show that it remains true for n. But how do we proceed? Let's express $n^3 - n$ in terms of $n - 1$.

$$n^3 - n = [(n-1)+1]^3 - [(n-1)+1] = (n-1)^3 + 3(n-1)^2 + 3(n-1) + 1 - (n-1) - 1$$

$$= (n-1)^3 - (n-1) + 3[(n-1)^2 + (n-1)] = 3k + 3[(n-1)^2 + (n-1)] = 3[k + (n-1)^2 + (n-1)]$$

7 Example 4

Prove that every integer can be expressed as the sum of **distinct** powers of 2.

When $n = 0$, we can express it as an empty sum (this sum contains no powers of 2 and therefore they are distinct). If this sounds a bit awkward, take the case when $n = 1$, which we can express as 2^0. Either one can serve as our base case. Now, for every $n > 0$, assume that the property holds up to $n - 1$ and show that it remains true for n. If n is odd, then $n - 1$ is even. Therefore, 2^0 cannot appear as a power of 2 in the sum for $n - 1$. But $n = (n - 1) + 2^0$ so we are done. But what if n is even? Then $n = 2 \times m$ where $m < n$. By multiplying by 2 all the powers of 2 in the sum for m we obtain n as a sum of distinct powers of 2.

8 Example 5

Given a pile of n blocks, prove that we need $n - 1$ splits to end up with n piles, each with exactly one block.

When $n = 1$, we need $0 = 1 - 1$ splits. This will serve as our base case. Now, for every $n > 1$, assume that the property holds up to $n - 1$ and show that it remains true for n. Given $n > 1$ blocks, we must perform a first split. This will split the pile into two piles of height k and $n - k$ for some $1 \leq k < n$. Therefore, $1 \leq n - k < n$ too. The two piles are now independent of each other, and we need $(k - 1) + (n - k - 1)$ splits to split the two piles. The total number of splits is

$$1 + (k - 1) + (n - k - 1) = n - 1$$

9 Example 6

Consider the same pile splitting problem above. But now every time we split a pile into two piles of height a and b, we receive ab points. Prove that the total number of points, regardless of how we split, is $n(n - 1)/2$.

When $n = 1$, we don't split and, therefore, we acquire $0 = 1(1 - 1)/2$ points. This will serve as our base case. Now, for every $n > 1$, assume that the property holds up to $n - 1$ and show that it remains true for n. Given $n > 1$ blocks, we must perform the first split. This will split the pile into two piles of height k and $n - k$ for some $1 \leq k < n$. Therefore, $1 \leq n - k < n$ too. We acquire $k(n - k)$ points from the first split. The two piles are now independent of each other, and we acquire $k(k - 1)/2$ points from splitting the first and $(n - k)(n - k - 1)/2$ points from splitting the second. The total number of points is

$$k(n - k) + \frac{k(k - 1)}{2} + \frac{(n - k)(n - k - 1)}{2} = \frac{n(n - 1)}{2}$$

Can you relate this problem to the handshaking problem?

10 Example 7

The Fibonacci numbers form an infinite sequence:

$$0 \quad 1 \quad 1 \quad 2 \quad 3 \quad 5 \quad 8 \quad 13 \quad 21 \quad 34 \quad 55 \quad 89 \quad \dots$$

The n^{th} (we start at 0) Fibonacci number is the sum of the $(n-1)^{st}$ and $(n-2)^{nd}$ Fibonacci numbers. Hence $F_n = F_{n-1} + F_{n-2}$ with $F_0 = 0$ and $F_1 = 1$. It is easy to obtain the n^{th} Fibonacci number for any n if we start with F_0 and F_1 and repeatedly add the last two entries. However, can we find an expression for F_n? This will be covered in the next topic on recurrences, but for now, we can prove by induction that (as I said before, induction can sometimes be useful but not insightful):

$$F_n = \frac{1}{\sqrt{5}}\Big[\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\Big]$$

Let $\phi = (1+\sqrt{5})/2$ and observe that $1-\phi = (1-\sqrt{5})/2$. When $n = 0$, $F_0 = [\phi^0 - (1-\phi)^0]/\sqrt{5} = 0$. When $n = 1$, $F_1 = [\phi^1 - (1-\phi)^1]/\sqrt{5} = (2\phi-1)/\sqrt{5} = 1$. Observe that we need both of these for our base case since every F_n is expressed in terms of the previous two (the inductive step below only works when $n > 1$ so our base cases must cover up to $n = 1$). Now for every $n > 1$, assume that the property holds up to $n-1$, and show that it remains true for n.

$$F_n = F_{n-1} + F_{n-2} = \frac{1}{\sqrt{5}}[\phi^{n-1} - (1-\phi)^{n-1}] + \frac{1}{\sqrt{5}}[\phi^{n-2} - (1-\phi)^{n-2}]$$

$$= \frac{1}{\sqrt{5}}\phi^n\Big[\frac{1}{\phi} + \frac{1}{\phi^2}\Big] - \frac{1}{\sqrt{5}}(1-\phi)^n\Big[\frac{1}{(1-\phi)} + \frac{1}{(1-\phi)^2}\Big]$$

Is it easy to verify that $1/\phi + 1/\phi^2 = 1$, the same holds for the term involving $(1-\phi)$: ϕ and $(1-\phi)$ are the two solutions for $x + 1 = x^2$. Therefore,

$$F_n = \frac{1}{\sqrt{5}}\Big[\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\Big]$$

11 Rules of thumb for induction

Here are some techniques to guide you when attempting to prove by induction.

- One inside the other: find the expression for $(n-1)$ "inside" the expression for n. This is often useful when dealing with a sum or a product of terms, say n of them. Examples 1 and 2 fall under this category.

- Side by side: Put the expression for $n-1$ and the expression for n side by side and see how you can get from one to another. Example 3 falls under this category.

- Case analysis on n: For instance, you might want to consider the case when n is even and the case when n is odd. Example 4 falls under this category.

- Make a move: This can break the problem into two similar and independent subproblems. Sometimes the move is general and represents a class of moves. Making a move usually establishes a recurrence (see below). Examples 5 and 6 fall under this category.

- Use a recurrence: A recurrence gives you the value of a function on n in terms of values of the function on smaller input, e.g. $n - 1$ and/or $n - 2$. This naturally guides the induction. Example 7 falls under this category.