Induction Proofs

CS 234

0 Introduction

This document contains examples of good proofs based on the induction activity completed in class. These are not the only ways to write good proofs.

These proofs may contain footnotes explaining different thought processes that occurred in their construction, to help show you how to think about writing proofs. Commentary may also be provided at the end about alternative approaches.

1 Proofs

Blue

```
def dbl(n):
    if n == 0:
        return 0
    else:
        return dbl(n-1) + 2
```

Theorem 1. $\forall n \in \mathbb{N}.\, dbl(n) = 2n$

Proof. The proof of this statement follows by induction over the natural numbers. For this purpose, let $P(n)$ be defined as $dbl(n) = 2n$. We now show both the base case and inductive case.

Base Case $n = 0$: For $n = 0$, we find that $P(n)$ means $dbl(0) = 2 \cdot 0$, which is of course 0. And because n is 0, the conditional statement in $dbl(n)$ will be true, so $dbl(n)$ will return 0.[1] Thus $P(0)$ holds.

Inductive Case: For the inductive hypothesis, assume $P(k)$ holds for an arbitrary natural number k, which means $dbl(k) = 2k$. We want to show that $dbl(k+1) = 2(k+1)$, which is of course equal to $2k + 2$.

Because $k + 1 > 0$, the conditional statement in $dbl(k+1)$ will be false, and $dbl(k+1)$ will return $dbl(k) + 2$, which is of course $2k + 2$ by the inductive hypothesis. This is what we wanted to show.

Conclusion: Because both the base case and inductive case hold, induction allows us to conclude $\forall n \in \mathbb{N}.\, dbl(n) = 2n$. □

[1] This is how I will write about what code will do. I could be more formal if I wanted, but this is perfectly sufficient.

Red

Theorem 2. *For any natural x, the value $x^3 - x$ is divisible by 6. That is,* $\forall x \in \mathbb{N}. \exists y \in \mathbb{Z}. x^3 - x = 6y$

Proof. This statement can be proven by induction, letting the inductive predicate $P(x)$ be defined as $\exists y \in \mathbb{Z}. x^3 - x = 6y$.

Base Case $x = 0$: For the base case, we want to show $P(0)$. That is,[2] we want to show that there is some $y \in \mathbb{Z}$ such that $0^3 - 0 = 6y$. The following algebraic[3] equalities show that picking $y = 0$ works.

$$0^3 - 0 = 0 = 6 \cdot 0$$

Inductive Case: Suppose for the inductive hypothesis that $P(k)$ holds for an arbitrary $k \in \mathbb{N}$. That is, suppose $k^3 - k = 6y$ for some $y \in \mathbb{Z}$.

We then want to show that $P(k+1)$ holds. That is, we want to show that $(k+1)^3 - (k+1) = 6z$ for some integer z.[4]

To show this statement, we first use the following chain of equalities:[5]

$$\begin{aligned}
(k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - k - 1 && \textit{algebra} \\
&= (k^3 - k) + 3(k^2 + k) && \textit{algebra} \\
&= 6y + 3(k^2 + k) && IH
\end{aligned}$$

To complete this proof, we must now show that $k^2 + k = 2u$ for some $u \in \mathbb{Z}$. That is, we must show that $k^2 + k$ is even. To do so, we case on whether k is even or odd.[6]

If k is even, then so is k^2, and thus so is $k^2 + k$. And if k is odd, then so is k^2, which leaves $k^2 + k$ even. Thus $k^2 + k$ is even.[7]

Since $k^2 + k$ is even no matter whether k is even or odd, $k^2 + k = 2u$ for some $u \in \mathbb{Z}$. This case can then be completed with the following equalities:

[2] I am using the phrase "that is" to indicate that I am about to explain the preceeding statement in more detail. Here that clearly means I am going to unwrap the definition, as $P(0)$ cannot be elaborated upon in any other way.

[3] I am using the qualifier "algebraic" here to indicate that the only steps I am taking in the chain of equalities are algebraic. I am not using any nontrivial identities or definitions.

[4] Notice that I changed the variable bound in the existential quantifier of P's definition from y to z. This is because I already used y above with $P(k)$, and I want to be able to pick a new number for this second use of the definition of P. In general, it is both acceptable and preferable to relabel variables in definitions like this so that you avoid variable name collisions.

[5] The goal here is to find the expression from $P(k)$ in the expression from $P(k+1)$. This can then be separated out and have the inductive hypothesis applied.

[6] While you could use induction to prove that all integers are either or odd, I will not make you do so. This is simple enough to assume.

[7] These even/odd properties are simple enough to assume. But you should be able to prove them more formally if you wanted to! I show you how after this proof.

$$\begin{aligned}(k+1)^3-(k+1) &= 6y+3(k^2+k) && \textit{above}\\ &= 6y+3(2u) && \textit{even def}\\ &= 6(y+u) && \textit{algebra}\end{aligned}$$

Because integers are closed under addition, $y+u$ is an integer, and therefore $(k+1)^3-(k+1)$ is divisible by 6 and $P(k+1)$ holds.

Conclusion: Thus, by induction, x^3-x has been shown to be divisible by 6 for any natural x. □

The proof part that cases over k being even or odd is written in a light-but-sufficient level of detail. However, there are other ways to write such proofs that are just as good. It is just important that the steps taken are clear without any big leaps of logic. If you were concerned about the level of detail, you could prove the same statement in more detail with the following:

If k is even, then $k=2v$ for some $v\in\mathbb{Z}$ by definition, and the following equalities hold:

$$\begin{aligned}k^2+k &= (2v)^2+(2v) && \textit{even def}\\ &= 4v^2+2v && \textit{algebra}\\ &= 2(2v^2+v) && \textit{algebra}\end{aligned}$$

As v is an integer, so is $2v^2+v$.[8] Thus k^2+k is twice an integer, i.e., is even.

If k is odd, then $k=2v+1$ for some $v\in\mathbb{Z}$ by definition, and the following equalities hold:

$$\begin{aligned}k^2+k &= (2v+1)^2+(2v+1) && \textit{even def}\\ &= 4v^2+4v+1+2v+1 && \textit{algebra}\\ &= 2(2v^2+3v+1) && \textit{algebra}\end{aligned}$$

As v is an integer, so is $2v^2+3v+1$. Thus k^2+k is twice an integer, i.e., is even.

[8] This is implicitly referencing that integers are closed under addition and multiplication. It is already plenty detailed for pointing out that we want to know whether the value is an integer. A proof can ignore this detail and still be a good proof.

Green

Theorem 3. *The number of words of length no greater than m over the alphabet a, b, and c is equal to $\frac{1}{2}(3^{m+1}-1)$.*

That is, $|\{w \in \{a,b,c\}^* \mid |w| \leq m\}| = \frac{1}{2}(3^{m+1}-1)$.

Proof. Let $P(m)$ be the statement that the number of words in $\{a,b,c\}^*$ of length at most m is $\frac{1}{2}(3^{m+1}-1)$.[9] Now induct with the following cases:[10]

Base Case $m = 0$: Note that ϵ is in $\{a,b,c\}^*$ and is the unique string of length 0. Moreover, we can calculate $\frac{1}{2}(3^{0+1}-1) = 1$. Thus $\frac{1}{2}(3^{0+1}-1)$ does correctly count the 1 string of size 0, and so $P(0)$ holds.[11]

Inductive Case: Assume for the inductive hypothesis that $P(k)$ holds for some k, so the number of words in $\{a,b,c\}^*$ of length less than or equal to k is $\frac{1}{2}(3^{k+1}-1)$.

There are 3^{k+1} words with $k+1$ letters because each letter in the word can be one of 3 choices (a, b, or c).

Adding these words of length $k+1$ to the set of words of length at most k gives the set of words of length at most $k+1$. The number of words in this set is $\frac{1}{2}(3^{k+1}-1)$ (by IH) plus 3^{k+1}.

$$\frac{1}{2}(3^{k+1}-1) + 3^{k+1} = \frac{1}{2}(3^{k+1} - 1 + 2 \cdot 3^{k+1}) = \frac{1}{2}(3^{k+2}-1)$$

Thus we can show algebraically that the set of words of length at most $k+1$ is $\frac{1}{2}(3^{k+2}-1)$, which satisfies $P(k+1)$

Conclusion Because we have shown both the base case for $m = 0$ and the inductive case, we can conclude $P(m)$ holds for all natural numbers $m \geq 0$. By definition, this is means, for all naturals m, that the number of words of length no greater than m over the alphabet a, b, and c is equal to $\frac{1}{2}(3^{m+1}-1)$, which is what we wanted to show. □

[9] You don't always need a fully mathematical predicate! It is nice to have a fully mathematical predicate, but sometimes you can do just fine with a slightly informal one. The trick is to use formality in ways that help to explain and clarify.

[10] I am purposefully writing this particular proof in such a way as to delay saying why I am doing each step. It will be illustrative to see the difference in how the proof feels.

[11] I chose to write this in a simpler, but still informative enough, style. I would not go much simpler than this.