Strong Induction Proofs From Lecture

CS 234

0 Introduction

This document contains examples of good proofs based on the strong induction lecture. 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

Frogs

A frog can hop across a line of lilypads by either making a small hop to the next lilypad or a big hop over the next lilypad to the one after that. Let $Ways(n)$ count the number of ways the frog can hop to the n^{th} lilypad.

The n^{th} Fibonacci number is given by $F(n)$, which is defined by the following recursive recurrence equation:

$$F(n) = \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ F(n-1) + F(n-2) & n \geq 2 \end{cases}$$

Theorem 1. $\forall n \in \mathbb{N}. Ways(n) = F(n+1)$

Proof. This proof proceeds by strong induction over the parameter n using the following inductive predicate:

$$P(n) := Ways(n) = F(n+1)$$

Base Case $n = 0$ To show that $Ways(0) = F(0+1)$, first consider the number of ways that the frog can not hop to any lilypad. This task can only be accomplished in one unique way by staying still and making no hops, so $Ways(0) = 1$.[1]

Now observe the following equalities:[2]

$$\begin{aligned} Ways(0) &= 1 && [stay\ still] \\ &= F(1) && [F\ def] \\ &= F(0+1) && [math] \end{aligned}$$

Thus $Ways(0) = F(0+1)$, and so $P(0)$ holds.

Base Case $n = 1$ To show that $Ways(1) = F(1+1)$, first consider the number of ways that the frog can hop to the first lilypad. This task can only be accomplished in one unique way by making a single small hop. Hopping with a big hop or making any more hops will overshoot, and not hopping at all will undershoot. Thus, $Ways(1) = 1$.

[1] One could also formalize this by considering each hop as a letter, like s for small hop and b for big. Then one could count the "weight" of strings of hops, 1 for every s and 2 for every b, and one would find that the only string with weight 0 is ϵ.

[2] The last line is a little pedantic. The fact that 0+1=1 is simple enough that it does not really need be made its own step. But I personally enjoy writing pedantically formal proofs, and I think it is somewhat instructive to see the precise substitutions being made.

Now observe the following equalities:

$$\begin{aligned}
Ways(1) =& 1 && [1\ small\ hop]\\
& 1+0 && [math]\\
=& F(1)+F(0) && [F\ def]\\
=& F(2-1)+F(2-2) && [math]\\
=& F(2) && [F\ def]\\
=& F(1+1) && [math]
\end{aligned}$$

Thus $Ways(1) = F(1+1)$, and so $P(1)$ holds.

Inductive Case Assume for the inductive hypothesis that, for some natural $n \geq 1$,[3] $P(k)$ holds for all $0 \leq k \leq n$. We want to show that $P(n+1)$ holds, i.e., that $Ways(n+1) = F((n+1)+1)$.

First observe that no hop sequence to the $(n+1)^{th}$ lilypad can be empty, as $n+1 > 0$. Second observe that every nonempty sequence of hops can mutually exclusively and exhaustively be classified into either those hops sequences that end in a small hop or those that end in a big hop. If the sequence ends in a small hop, then all the hops prior get the frog to lilypad n, and there are $Ways(n)$ such sequences. Alternatively, if the sequence ends in a big hop, then all the hops prior get the frog to lilypad $n-1$, and there are $Ways(n-1)$ such sequences. Because those two options are mutually exclusive and exhaustive, we can therefore conclude that $Ways(n+1) = Ways(n) + Ways(n-1)$.[4]

Now observe the following equalities.

$$\begin{aligned}
Ways(n+1) =& Ways(n) + Ways(n-1) && [small\ or\ big\ ending]\\
=& F(n+1) + F((n-1)+1) && [IH]\\
=& F((n+2)-1) + F((n+2)-2) && [math]\\
=& F(n+2) && [F\ def]\\
=& F((n+1)+1) && [math]
\end{aligned}$$

The inductive hypothesis can apply in the above equalities because we find that $n-1$ and $(n-1)+1$ satisfy $0 \leq n-1 \leq (n-1)+1 = n$, so both cases fall into the assumed range.[5]

Thus $Ways(n+1) = F((n+1)+1)$, and so $P(n+1)$ holds.

[3] The variable n was chosen to be the largest shown base case. This is important; we want all of the base cases to be considered for inductive step in strong induction. The case's argument would also not work if n was 0 because we would undershoot the smallest base cases.

[4] This is not the first time I have done this in this proof, but do note that this was an argument given in English. Those are ok to make, so long as what needs to be explained is explained clearly.

[5] This is a little pedantic, but good practice to check. I have seen many proofs go wrong by using cases outside of the range. Checking this will also tell you if you have selected enough base cases—if you need a case outside the range, then you need more base cases!

Conclusion Thus, by strong induction, we can conclude that $\forall n \in \mathbb{N}.\, P(n)$, i.e., $\forall n \in \mathbb{N}.\, Ways(n) = F(n+1)$.

□

Primes

Let $m \mid n$ mean that the natural number m divides n, i.e., that $\exists z \in \mathbb{Z}.\, m \cdot z = n$.
Let $Prime(n)$ mean that the natural number n is prime, i.e., that
$n > 1 \wedge \forall\, 1 < m < n.\, \neg(m \mid n)$.[6]

Theorem 2. $\forall n \in \mathbb{N}.\, n > 1 \rightarrow \exists p \in \mathbb{N}.\, Prime(p) \wedge p \mid n$

Proof. This proof proceeds by string induction over the parameter n using the following inductive predicate:[7]

$$Q(n) := \exists p \in \mathbb{N}.\, Prime(p) \wedge p \mid n$$

Base Case $n = 2$ To show that $Q(2)$ holds, first observe that $Prime(2)$ holds because $2 > 1$ and there are no such naturals m strictly between 1 and 2 so the universal quantifier in $Prime$'s definition is satisfied vacuously.[8] Then observe that $2 = 1 \cdot 2$, so picking $z = 1$ witnesses that $2 \mid 2$ by definition. These two observations satisfy both conjuncts of $Q(2)$ where $p = 2$, and thus this case is complete.

Inductive Case Assume for the inductive hypothesis that, for some $n \geq 2$, $P(k)$ holds for all $2 \leq k \leq n$. We now want to show $P(n+1)$, and to do so we case on whether $Prime(n+1)$.

Subcase $Prime(n+1)$ If $Prime(n+1)$, then observe that $n+1 = 1 \cdot (n+1)$ so picking $z = 1$ witnesses that $n+1 \mid n+1$ by definition. Thus $n+1$ witnesses that $Q(n+1)$ holds in this case. [9]

Subcase $\neg Prime(n+1)$ If $\neg Prime(n+1)$, negating the definition of $Prime$ yields that $n+1 \leq 1 \vee \exists\, 1 < m < n+1.\, m \mid n+1$. For any natural $n \geq 2$, it is the case that $n+1 > 1$, so the first disjunct cannot hold. It must therefore be that the second disjunct holds and $\exists\, 1 < m < n+1.\, m \mid n+1$.

Let m be the natural number dividing $n+1$ that the true disjunct guarantees

[6] This may be different from definitions of primes that you have seen before, but it is equivalent.

[7] I did not include $n > 1$ in the predicate. This is because I will only induct starting from the base case 2, so the predicate will only be shown for $n > 1$.

[8] This might be new terminology, but its idea follows from what we already know about quantifiers and implications. $\forall 1 < m < 2.R(m)$ is just shorthand for $\forall m.1 < m < 2 \rightarrow R(m)$, and the "vacuous" satisfaction of this statement is just that the lefthand side of the implication is false.

[9] I'm varying my wording a little just to show that you can.

to exist. Then observe the following identities:[10][11]

$$\begin{aligned} n+1 =& z \cdot m \text{ (for some } z) && [m \mid n \; def] \\ =& z \cdot (z' \cdot p) \text{ (for some } z', p \text{ s.t. } Prime(p)) && [IH, 2 \leq m \leq n] \\ =& (z \cdot z') \cdot p && [math] \end{aligned}$$

Since $n+1 = (z \cdot z') \cdot p$ for some integers p, z, z', the product $z \cdot z'$ witnesses that $p \mid n+1$. And since $Prime(p)$, it then follows by definition that $Q(n+1)$ holds in this case.

Conclusion Thus, by strong induction, it follows that $\forall n \in \mathbb{N}. n > 1 \rightarrow Q(n)$, i.e., $\forall n \in \mathbb{N}. n > 1 \rightarrow \exists p \in \mathbb{N}. \, Prime(p) \wedge p \mid n$.

□

[10] To make the reasoning smoother, I introduce existentially quantified variables in my line-by-line mathematics by writing "for some" after them in parenthesis. This makes it clear where each variable is coming from and how it is quantified without interrupting the flow of the reasoning.

[11] In this line-by-line reasoning, I justify the IH application by using my end-of-line justification to point out that m falls within the assumed range.