CMPSCI 250: Introduction to Computation

Lecture #18: Variations on Induction for Naturals
David Mix Barrington
3 March 2014

Variations on Induction

- Not Starting at Zero
- Justifying the "Start Anywhere" Rule
- Induction on the Odds or the Evens
- Strong Induction
- The Law of Strong Induction
- Example: Existence of a Factorization
- Example: Making Change

Not Starting at Zero

- Last lecture we claimed "for any n, the n'th odd number is 2n-1" but we *didn't* prove this by induction.
- The reason was that given our Law of Mathematical Induction, we would need to prove P(0), which says "the 0'th odd number is -1", and this doesn't make much sense.
- Of course the statement P(1) says "the first odd number is 1", which is true.

Not Starting at Zero

- Also, the inductive case is fine -- if we assume that the n'th odd number is $2n - 1$, then clearly the n+1'st odd number should be two greater, or $(2n - 1) + 2 = 2(n + 1) - 1$.
- It seems reasonable to have a Law of Start Anywhere Induction that says "if you prove $P(k)$ for any integer k, and prove $\forall n: ((n \geq k) \wedge P(n)) \rightarrow P(n+1)$, you may conclude $\forall n: (n \geq k) \rightarrow P(n)$".

Digression: Bounded Quantifiers

- Suppose I have variables whose type is "natural", but I want to quantify over only the naturals that are at least 3.
- This works differently depending on the quantifier.
- If I say "there exists a natural that is at least 3" in symbols, this is "$\exists x: (x \geq 3) \wedge \ldots$"
- But to say "for every number that is at least 3, we write "$\forall x: (x \geq 3) \rightarrow \ldots$"

Justifying "Start Anywhere"

- Using the intuition about dominoes, for example, the Start Anywhere Rule is just as convincing as the ordinary rule.
- If we push over the k'th domino, and every domino at or after the k'th pushes over the next one, every domino after the k'th will eventually be pushed over.
- But it would be nice to know that we don't need a new axiom, so we will prove the Start Anywhere rule by ordinary mathematical induction.

Justifying "Start Anywhere"

- Suppose we have a predicate P(x), for integer x, and we have proved P(k) and $\forall x: ((x \geq k) \wedge P(x)) \rightarrow P(x+1)$ for some integer k.
- For any natural n, we define a new predicate Q(n) to be P(k+n).
- Now we will prove the statement $\forall n: Q(n)$ by ordinary induction.

Justifying "Start Anywhere"

- Q(0) is the statement P(k), which we are given.
- For the inductive step, we assume Q(n) which is P(k+n). We specify the other premise to x = k + n, giving the statement "$(k + n \geq k) \wedge P(k+n)) \rightarrow P(k+n+1)$".
- Since n is a natural, $k + n \geq k$ is true, so we get P(k+n+1) which is the same as Q(n+1). The ordinary induction is done.

More on “Start Anywhere”

- Having proved ∀n: Q(n) by ordinary induction, we can translate it back into terms of P as ∀n: P(k +n), which means that P is true for all arguments k or greater. This is the conclusion of the Start Anywhere Rule.
- Another way to think about this is that we are doing induction on a *new* inductively defined type, in this case “integers that are ≥ k”. This type could be defined as what we get by starting from k and taking successors, and the fact that it contains nothing else is our induction rule.

More on “Start Anywhere”

- If k is positive, we can also prove the “Start at k Rule” by ordinary induction in another way.
- Let Q(n) be the predicate “$(n \geq k) \rightarrow P(n)$”. Then Q(0) is true, and we can prove $\forall n: Q(n) \rightarrow Q(n+1)$ by cases.
- If $n < k$ we can use Vacuous Proof. If $n = k$ we use our premise P(k). And if $n > k$, Q(n) gives us P(n), and we can use Specification on the other premise to give us P(n+1).

Clicker Question #1

- "If X is a convex polygon with k sides, then X can be divided into exactly k - 2 triangles by drawing lines among its vertices." If I wanted to prove this (true) geometry fact for all k by induction, what should be my starting point?
- (a) k = 3
- (b) k = 2
- (c) k = 1
- (d) k = 0

Answer #1

- "If X is a convex polygon with k sides, then X can be divided into exactly k - 2 triangles by drawing lines among its vertices." If I wanted to prove this (true) geometry fact for all k by induction, what should be my starting point?
- *(a) k = 3*
- (b) k = 2
- (c) k = 1
- (d) k = 0

Induction on the Odds or Evens

- The first several odd perfect squares: 1, 9, 25, 49, and 81, are all congruent to 1 modulo 8. It's easy to prove by modular arithmetic that every odd number satisfies $n^2 \equiv 1 \pmod{8}$, but suppose we want to prove this by induction?
- We now know how to start at $n = 1$ rather than $n = 0$, but our inductive step poses a different problem. We can't say that $n^2 \equiv 1$ for even n, because it isn't true.

Induction on the Odds or Evens

- If we let P(n) be "if n is odd, then $n^2 \equiv 1 \pmod 8$", then P(n) is true for all n, but the inductive hypothesis won't help us in a proof because it is true vacuously -- it says nothing about n^2 that we could use for $(n+1)^2$.
- We can easily prove $P(n) \rightarrow P(n+2)$, however, and this looks like the correct inductive step for a statement about just the odds or just the evens.

Induction on the Odds or Evens

- We have another new induction rule: "If k is odd, P(k) is true, and ∀n: (P(n) ∧ (n is odd) ∧ (n ≥ k)) → P(n+2) is true, then ∀n: ((n is odd) ∧ (n ≥ k)) → P(n) is true."
- Of course there is a similar rule for the evens.
- As before, we can prove the validity of these rules by ordinary induction.

Clicker Question #2

- "If n is a natural and $n \equiv 3 \pmod 5$, then $n^2 + 1 \equiv 0 \pmod 5$." If I want to prove this fact by induction, how should I do it?
- (a) base P(0), induction P(n) → P(n+1)
- (b) base P(3), induction P(n) → P(n+1)
- (c) base P(3), induction P(n) → P(n+5)
- (d) base P(5), induction P(n) → P(n+3)

Answer #2

- "If n is a natural and $n \equiv 3 \pmod 5$, then $n^2 + 1 \equiv 0 \pmod 5$." If I want to prove this fact by induction, how should I do it?
- (a) base P(0), induction P(n) → P(n+1)
- (b) base P(3), induction P(n) → P(n+1)
- *(c) base P(3), induction P(n) → P(n+5)*
- (d) base P(5), induction P(n) → P(n+3)

Strong Induction

- The difficulty of ordinary induction in this last case was that the truth of P(n+1) depended on P(n-1) rather than on P(n), so that the premise of the ordinary inductive step P(n) → P(n+1) gave no help.
- If we return to the domino metaphor, all we actually care about is that every domino is knocked over, whether by the preceding domino or some other earlier one.

Strong Induction

- We can modify our Law of Induction to get a new Law of Strong Induction, which will handle these situations. The new law will work in any situation where the old one will, so we could just use it automatically.
- But in the many situations where ordinary induction works, using it makes for a clearer proof. So if we don't recognize the need for strong induction immediately, we start an ordinary induction proof and convert it in midstream if necessary.

The Law of Strong Induction

- The Law of Strong Induction is as follows:
- Given a predicate $P(n)$, define $Q(n)$ to be the predicate $\forall i: (i \leq n) \rightarrow P(i)$.
- Then if we prove both $P(0)$ and $\forall n: Q(n) \rightarrow P(n+1)$, we may conclude $\forall n: P(n)$.
- We'll now justify this formally by using ordinary induction.

The Law of Strong Induction

- The reason this is valid is that those two steps are exactly what we need for an ordinary induction proof of $\forall n: Q(n)$.
- $Q(0)$ and $P(0)$ are the same statement, and $Q(n+1)$ is equivalent to $Q(n) \wedge P(n+1)$.
- So $Q(n) \rightarrow P(n+1)$ allows us to derive $Q(n) \rightarrow Q(n+1)$, the inductive step of our ordinary induction. (And of course $\forall n: Q(n)$ implies $\forall n: P(n)$.)

Using Strong Induction

- In practice, this means that if in the middle of an ordinary induction we decide that Q(n) would be a more useful inductive hypothesis than P(n), we just assume it, retroactively converting the proof to a strong induction.
- There is nothing that we need to add to our conclusion, as by proving P(n+1) we also prove Q(n+1).

Existence of a Factorization

- Let P(n) be the statement "n can be written as a product of prime numbers".
- We have asserted that this P(n) is true for all positive n (0 cannot be written as such a product). Our "proof" has been a recursive algorithm that generates a sequence of primes that multiply to n.
- Now with Strong Induction (starting from 1 rather than 0) we can make this idea into a formal proof.

Existence of a Factorization

- We begin by noting that P(1) is true, since 1 is the product of an empty sequence of primes.
- Now we let Q(n) be the statement "((i ≥ 1) ∧ (i ≤ n)) → P(i)". We can finish the strong induction by proving the strong inductive step ∀n: ((n ≥ 1) ∧ Q(n)) → P(n+1).
- (We need the "(n ≥ 1)" so we are not asked to deal with the false statement P(0).)

Existence of a Factorization

- But this proof is easy! Let n be an arbitrary positive natural. If n+1 is prime, P(n+1) is true because n+1 is the product of itself.
- Otherwise, by the definition of primality, n+1 = a × b where a and b are each in the range from 2 to n. Since a ≤ n and b ≤ n, each can be written as a product of primes by the strong IH. And multiplying these two sequences gives us one for n+1.

Clicker Question #3

- "If $n \geq 1$, the number of tests needed for binary search on a list of length n is the ceiling of $\log_2 n$." To prove this by induction *on n*, I will use the fact that one test at worst reduces the size of my search to (n-1)/2 (Java division). What steps do I need for my strong induction?
- (a) base P(1), induction $P(k) \rightarrow P(k+1)$
- (b) base P(1), induction $P(k) \rightarrow P(2k)$
- (c) base P(1), induction $P(k) \rightarrow P(2k) \wedge P(2k+1)$
- (d) base P(1) and P(2), induction $P(k) \rightarrow P(k+2)$

Clicker Question #3

- "If $n \geq 1$, the number of tests needed for binary search on a list of length n is the ceiling of $\log_2 n$." To prove this by induction *on n*, I will use the fact that one test at worst reduces the size of my search to (n-1)/2 (Java division). What steps do I need for my strong induction?
- (a) base P(1), induction P(k) → P(k+1)
- (b) base P(1), induction P(k) → P(2k)
- *(c) base P(1), induction P(k) → P(2k) ∧ P(2k+1)*
- (d) base P(1) and P(2), induction P(k) → P(k+2)

Example: Making Change

- Suppose I have \$5 and \$12 gift certificates, and I would like to be able to give someone a set of certificates for any integer number of dollars.
- I clearly can't do \$4 or \$11, but if the amount is large enough I should be able to do it. By trial and error (or more cleverly) you can show that \$43 is the last bad amount.

Example: Making Change

- Let P(n) be the statement "\$n can be made with \$5's and \$12's".
- I'd like to prove $\forall n: (n \geq 44) \rightarrow P(n)$ by strong induction, starting with P(44).
- It's easy to prove $\forall n: P(n) \rightarrow P(n+5)$, which helps with the strong inductive step, namely $\forall n: Q(n) \rightarrow P(n+1)$, where Q(n) is the statement $\forall i:((i \geq 44) \wedge (i \leq n)) \rightarrow P(i)$.

Example: Making Change

- So let n be arbitrary and assume Q(n). If $n \geq 48$, Q(n) includes P(n-4), and I can prove P(n+1) from P(n-4). But there are the cases of P(45), P(46), P(47), and P(48) which I have to do separately. One way to think of this is that with an inductive step of $P(n) \rightarrow P(n+5)$, I need five base cases.
- If my sum proving P(n) had at least two \$12's, I could replace them with five \$5's and get the inductive step for an ordinary induction.