Inductive Proof

Class 30

Introduction

- recursion is an extremely powerful programming technique
- many things that are difficult to express iteratively are easy to express recursively
- but if we are to trust that recursion works as intended, we need to be able to reason formally about it
- one way of doing so is by mathematical induction

- induction and recursion are two sides of the same coin

Sum of Squares

- one question on the last assignment was to write a program to calculate the sum of squares of the first n positive integers
- most of you wrote a program that corresponded to this formulation:

$$\text{sumsq}(n) = \begin{cases} 1 & \text{if } n = 1 \\ \text{sumsq}(n-1) + n^2 & \text{otherwise} \end{cases}$$

- but at least one of you gave the following program:

$$\text{sumsq}(n) = \frac{n(n+1)(2n+1)}{6}$$

- these are radically different formulations, one recursive, one not
- you can easily check a few examples, but is either one correct for all positive integers? i.e., are they equivalent
- and if so, can you prove it?

Mathematical Induction

- note that any non-empty subset of the natural numbers has a least element based on less-than
- this is the same as saying that every descending chain of natural numbers is finite: the naturals are a well-founded poset

- suppose we wish to prove some predicate $P(n)$ is true for all natural numbers $n \geq m$ where m is some specified natural value (usually m is 0 or 1)

- the principle of mathematical induction states that we can do so in just two steps:
  1. prove $P(m)$ is true directly
  2. assume $P(k)$ is true for an arbitrary $k > m$, and use this to prove that $P(k + 1)$ is true

Sum of Squares

- recall the claim above

$$\text{sumsq}(n) = \frac{n(n+1)(2n+1)}{6}$$

- if this is true, that means

$$1 + 4 + 9 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

- let $P(n)$ denote the above equation and let $m = 1$
- to prove it using mathematical induction, we have to perform the two steps

Step 1

- prove $P(m)$ directly where $m = 1$

$$\begin{aligned} 1 &= \frac{1(1+1)(2(1)+1)}{6} \\ &= \frac{1(2)(3)}{6} \\ &= 1 \end{aligned}$$

- this is true, so step 1 is done
- step 1 is usually more a “verification” than a “proof”

Step 2

- assume $P(k)$ is true for an arbitrary $k > m$, and use this to prove that $P(k+1)$ is true
- using the assumption, we have $P(k+1)$

$$
\begin{aligned}
&1 + 4 + \cdots + k^2 + (k+1)^2 \\
&\qquad = (1 + 4 + \cdots + k^2) + (k+1)^2 && \text{associate} \\
&\qquad = \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \text{assumption} \\
&\qquad = \frac{[k+1]([k+1]+1)(2[k+1]+1)}{6} && \text{algebra}
\end{aligned}
$$

- expression (3) is exactly $P(k+1)$, and thus step 2 is done

- the principle of mathematical induction allows us to state that we have now proved for all positive integers n

$$1 + 4 + 9 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Recursive Sum of Squares

- the student who submitted the Prolog program above submitted a correct program
- what about the students who submitted the recursive program?

$$\text{sumsq}(n) = \begin{cases} 1 & \text{if } n = 1 \\ \text{sumsq}(n-1) + n^2 & \text{otherwise} \end{cases}$$

- we can use a very similar mathmatical induction argument to show that this is also correct and computes the same value
- let $P(n)$ be the statement $\text{sumsq}(n) = 1 + 4 + 9 + \cdots + n^2$ for all $n > 0$

- step 1, let $m = 1$ and verfify that $1 = 1$ and so the statment is correct

Step 2

- assume $f(k)$ is true and use that to prove $f(k+1)$ is true

$$\begin{aligned} f(k+1) &= f([k+1]-1)+(k+1)^2 && \text{definition of } f \\ &= f(k)+(k+1)^2 && \text{algebra} \\ &= 1+4+9+\cdots+k^2+(k+1)^2 && \text{assumption} \\ &= 1+4+9+\cdots+(k+1)^2 && (4) \end{aligned}$$

- expression (4) is the rhs of $f(k+1)$, and so the statement is proved correct for all integers greater than 0

Well-Foundedness

- mathematical induction works because the naturals are a well-founded poset
- recursion works from an arbitrary starting point backwards down the descending chain to the base case minimal element
- induction works by showing the proposition is true for the base case and by showing that the recursive step between two arbitrary elements is valid
- and therefore it is valid for the entire descending chain from an arbitrary element down to the base case

- therefore mathematical induction, and recursion, can be used on any well-founded poset