CSC236 fall 2012

structural induction

Danny Heap
heap@cs.toronto.edu
BA4270 (behind elevators)
http://www.cdf.toronto.edu/~heap/236/F12/
416-978-5899

Using Introduction to the Theory of Computation, Chapter 4, Section 1.1

Outline

Equivalence of inductions

Structural induction

Notes

WO $\Rightarrow$ MI $\Rightarrow$ CI $\Rightarrow$ WO

The cycle is proved in the text, here is one link. Suppose you believe MI, and you have shown for some property P:

$$\forall n \in \mathbb{N}, (\forall 0 \leq i < n, P(i)) \Rightarrow P(n) \tag{1}$$

Now define a slightly different predicate:
$P'(n) : \forall 0 \leq i \leq n, P(i)$, in other words, $P(i)$ is true up to and including n. Using only MI prove $\forall n, P'(n)$:

Base case: Since we showed (1), and there are no natural numbers smaller than 0, we have $P'(0)$.

Induction step: Assume n is an arbitrary natural number and that $P'(n)$ is true. It follows from (1) that $P(n+1)$ is true, and hence $P'(n+1)$ is true.

Define sets inductively

...so as to use induction on them later

One way to define the natural numbers:

$\mathbb{N}$: The **smallest** set such that

1. $0 \in \mathbb{N}$
2. $n \in \mathbb{N} \Rightarrow n + 1 \in \mathbb{N}$.

By **smallest** I mean $\mathbb{N}$ has no proper subsets that satisfy these conditions. If I leave out **smallest**, what other sets satisfy the definition?

What can you do with it?

The definition on the previous page defined the simplest natural number (0) and the rule to produce new natural numbers from old (add 1). Proof using Mathematical Induction work by showing that 0 has some property, and then that the rule to produce natural numbers preserves the property, that is

1. Prove $P(0)$
2. Prove that $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$.

Other structurally-defined sets

Define $\mathcal{E}$: The **smallest** set such that

- $x, y, z \in \mathcal{E}$
- $e_1, e_2 \in \mathcal{E} \Rightarrow (e_1 + e_2), (e_1 - e_2), (e_1 \times e_2)$, and $(e_1 \div e_2) \in \mathcal{E}$.

Form some expressions in $\mathcal{E}$. Count the number of variables (symbols from $\{x, y, z\}$) and the number of operators (symbols from $\{+, \times, \div, -\}$). Make a conjecture.

Structural induction

$P(e): \ \mathrm{vr}(e) = \mathrm{op}(e) + 1$

To prove that a property is true for all $e \in \mathcal{E}$, parallel the recursive set definition:

- **Base case:** Show that the property is true for the simplest members, $\{x, y, z\}$
- **Induction step:** Show "inheritance": if $P(e_1)$ and $P(e_2)$, then all possible combinations $(e_1 + e_2)$, $(e_1 - e_2)$, $(e_1 \times e_2)$, and $(e_1 \div e_2)$ have the property.

Conclude that the property is true of all elements of $\mathcal{E}$.

Structural induction

$P(e): \ \mathrm{vr}(e) = \mathrm{op}(e) + 1$

Prove $\forall e \in \mathcal{E}, P(e)$

More structural induction

$(x + (y + (z + (x \div y))))$ $\quad h(x) = 0$

Define the height of x, y, or z as 0, and $\mathrm{h}((e_1 \odot e_2))$ as $1 + \max(\mathrm{h}(e_1), \mathrm{h}(e_2))$, if $e_1, e_2 \in \mathcal{E}$ and $\odot \in \{+, \times, \div, -\}$.

What's the connection between the number of variables and the height?

$h((x \div y)) = 1$

$h((x \div (y \times z))) = 2$

$((x+y) - (y \div z))$

even/odd rule

$vr(e) \geq 1 + h(e)$

$\log_2 \lceil vr(e) \rceil = h(e)$

$vr(e) \leq 2^{h(e)}$

More structural induction

$P(e) : \mathrm{vr}(e) \leq 2^{\mathrm{h}(e)}$

- verify for basis
  basis case $\{x, y, z\}$

- induction step
  assume $e_1, e_1 \in \mathcal{E}$ and
  that $P(e_1)$, $P(e_2)$ hold. Must
  show $P((e_1 \odot e_2))$ is
  true.

Recursive definition

Fibonacci sequence

This sequence comes up in applied rabbit breeding, the height of AVL trees, and the complexity of Euclid's algorithm for the GCD:

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

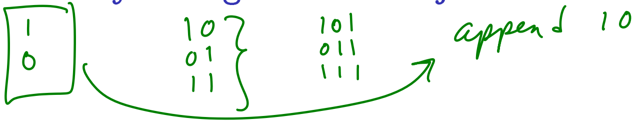
What is the sum of n Fibonacci numbers?

Fibonacci numbers

What is $\sum_{i=0}^{i=n} F(i)$?

Number of binary strings **without** adjacent 0s

0	1
1	2
2	3
3	5
4	8
5	



This is easy when $n = 0$ or $n = 1$. For $n > 1$ we have the possibility that the last bit added creates a forbidden 00.

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

The formula turns out to be related to $F(n)$, and it has the same annoying property $F(n)$ using the definition requires about n calculations.

$$G(3895) = G(3893) + G(3894)$$

Not closed form!

Closed form for $F(n)$?

No rabbit, no hat

The course notes present a proof by induction that

$$F(n) = \frac{\phi^n - \left(\hat{\phi}\right)^n}{\sqrt{5}}, \quad \phi = \frac{1+\sqrt{5}}{2}, \hat{\phi} = \frac{1-\sqrt{5}}{2}$$

You can, and should, be able to work through the proof. The question remains, why did somebody think of ϕ and $\hat{\phi}$?

Closed form

... without rabbits

0, 1, 1, 2, 3, 5, 8, 13, 21

wishful thinking $F(n) \approx r^n$

$\tilde{F}(n) = \tilde{F}(n-1) + \tilde{F}(n-2)$

Start with the idea that $F(n)$ seems to increase by something close to a fixed ratio. Let's try calling that r, and r has to satisfy:

$$r^n = r^{n-1} + r^{n-2} \Rightarrow r^2 = r + 1$$

There are two solutions to the quadratic equation: ϕ and $\hat{\phi}$, but what about the $1/\sqrt{5}$ factor?

$1 \cdot \phi^n$ $\frac{1+\sqrt{5}}{2}$ $\frac{1-\sqrt{5}}{2}$

If ϕ and $\hat{\phi}$ are solutions, so are linear combinations:

$$\alpha\phi^n + \beta\hat{\phi}^n = \alpha\phi^{n-1} + \beta\hat{\phi}^{n-1} + \alpha\phi^{n-2} + \beta\hat{\phi}^{n-2}$$

Rabbits, hats

$$\alpha = \frac{1}{\phi - \hat{\phi}}$$

Match up α and β to solutions:

$$\begin{aligned} \alpha\phi^0 + \beta\hat{\phi}^0 &= 0 \quad \Rightarrow \alpha = -\beta \\ \alpha\phi^1 + \beta\hat{\phi}^1 &= 1 \quad \Rightarrow \alpha(\phi - \hat{\phi}) = 1 \end{aligned}$$

Notes