CSC236 fall 2018

structural induction, well ordering

Danny Heap
heap@cs.toronto.edu / BA4270 (behind elevators)
http://www.teach.cs.toronto.edu/~heap/236/F18/
416-978-5899

Using Introduction to the Theory of Computation, Section 1.2–1.3

Computer Science
UNIVERSITY OF TORONTO

Outline

Structural induction

Well-ordering

Define sets inductively

...so as to use induction on them later!

E.g., 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 two 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. show that $P(0)$ is true for basis, 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:

verify base case(s): Show that the property is true for the simplest members, $\{x, y, z\}$, that is show $P(x)$, $P(y)$, and $P(z)$.

inductive step: Let e_1 and e_2 be arbitrary elements of $\mathcal{E}$. Assume $H(\{e_1, e_2\}) : P(e_1)$ and $P(e_2)$, that is e_1 and e_2 have the property.

show that $C(\{e_1, e_2\})$ follows: All possible combinations of e_1 and e_2 have the property, that is $P((e_1 + e_2))$, $P((e_1 - e_2))$, $P((e_1 \times e_2))$, and $P((e_1 \div e_2))$.

Structural induction

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

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

More structural induction

Define the heights, $h(x) = h(y) = h(z) = 0$, 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?

More structural induction

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

Well-ordering example

$\forall n, m \in \mathbb{N}, n \neq 0,\ R = \{r \in \mathbb{N} \mid \exists q \in \mathbb{N}, m = qn + r\}$ has a smallest element

This is the main part of proving the existence of a unique quotient and remainder:

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N} - \{0\}, \exists q, r \in \mathbb{N}, m = qn + r \wedge 0 \leq r < n$$

The course notes use Mathematical Induction. Well-ordering is shorter and clearer.

Principle of well-ordering

Every non-empty subset of $\mathbb{N}$ has a smallest element

Is there something similar for $\mathbb{Q}$ or $\mathbb{R}$?

For a given pair of natural numbers $m, n \neq 0$ does the set R satisfy the conditions for well-ordering?

$$R = \{r \in \mathbb{N} \mid \exists q \in \mathbb{N}, m = qn + r\}$$

If so, we still need to be sure that the smallest element, r' has

1. $0 \leq r' < n$
2. That q' and r' are unique — no other natural numbers would work

...in order to have

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N} - \{0\}, \exists! q', r' \in \mathbb{N}, m = q'n + r' \wedge 0 \leq r' < n$$

$\forall m \in \mathbb{N}, \forall n \in \mathbb{N} - \{0\}, \exists q, r \in \mathbb{N}, m = qn + r \wedge 0 \leq r < n$

Use: every non-empty subset of $\mathbb{N}$ has a smallest element

$\forall m \in \mathbb{N}, \forall n \in \mathbb{N} - \{0\}, \exists q, r \in \mathbb{N}, m = qn + r \wedge 0 \leq r < n$

Use: every non-empty subset of $\mathbb{N}$ has a smallest element

$P(n)$: Every round-robin tournament with n players with a cycle has a 3-cycle

Use: every non-empty subset of $\mathbb{N}$ has a smallest element

Claim: $\forall n \in \mathbb{N} - \{0, 1, 2\}, P(n)$.

If there is a cycle $p_1 > p_2 > p_3 \ldots > p_n > p_1$, can you find a shorter one?

Every non-empty subset of $\mathbb{N}$ has a smallest element

$P(n)$: Every round-robin tournament with n players that has a cycle has a 3-cycle

Claim: $\forall n \in \mathbb{N} - \{0, 1, 2\}, P(n)$.

Every non-empty subset of $\mathbb{N}$ has a smallest element

$P(n)$: Every round-robin tournament with n players that has a cycle has a 3-cycle

Notes