BCH ?
questions ?

CSC236 fall 2016

structural induction, well ordering

Danny Heap
heap@cs.toronto.edu / BA4270 (behind elevators)
http://www.cdf.toronto.edu/~csc236h/fall/
416-978-5899

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

Outline

Structural induction

Well-ordering

Define sets inductively

…so as to use induction on them later1

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? $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}$

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

simple induction

Other structurally-defined sets

$x, y, z \in \mathcal{E}$ $\quad$ $(x+y) \in \mathcal{E}$

$((x+y) \times z)$ $\quad$ $(x-y) \in \mathcal{E}$

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.

$\forall e \in \mathcal{E}, \quad vr(e) = op(e) + 1$

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:

$\odot \in \{+, -, \times, \div\}$

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

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

$xy \notin \mathcal{E}$

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

Verify base cases: Let $e \in \{x, y, z\}$. Then $vr(e) = 1$ and $op(e) = 0$, so $vr(e) = op(e) + 1$ and $P(e)$ holds.

Inductive step: Let $e_1, e_2 \in \mathcal{E}$. Assume $H(\{e_1, e_2\})$: $P(e_1) \wedge P(e_2)$, that is $vr(e_1) = op(e_1) + 1 \wedge vr(e_2) = op(e_2) + 1$.
Must show $C(\{e_1, e_2\})$: if $\odot \in \{+, -, \times, \div\}$ then $P((e_1 \odot e_2))$

$$\begin{aligned} vr((e_1 \odot e_2)) &= vr(e_1) + vr(e_2) && \text{\# same variables} \\ &= \underbrace{op(e_1) + 1 + op(e_2)}\ + 1 && \text{\# By } H(\{e_1, e_2\}) \\ &= op((e_1 \odot e_2)) + 1 && \text{\# added } \odot \text{ operator} \end{aligned}$$

That is $P((e_1 \odot e_2))$, i.e. $C(\{e_1, e_2\})$ holds.

More structural induction

nested-ness

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?

$$(\underbrace{(\overbrace{(x+y)}^{1} \div \overbrace{(x-y)}^{1})}_{2} + x)$$

3

Conjecture.

$\forall e \in \mathcal{E}, \quad vr(e) \leq 2^{h(e)}$

More structural induction

$P(e): \mathrm{vr}(e) \leq 2^{\mathrm{h}(e)}$ Proof by structural induction.

Verify base case: (exercise)

Inductive step Let $e_1, e_2 \in \mathcal{E}$. assume $H(\{e_1, e_2\})$: $P(e_1)$ and $P(e_2)$, that is $\mathrm{vr}(e_1) \leq 2^{h(e_1)}$ and $\mathrm{vr}(e_2) \leq 2^{h(e_2)}$.

Must show $C(\{e_1, e_2\})$: if $\odot \in \{+, -, \times, \div\}$ then $\mathrm{vr}((e_1 \odot e_2)) \leq 2^{h((e_1 \odot e_2))}$

$$
\begin{aligned}
\mathrm{vr}((e_1 \odot e_2)) &= \mathrm{vr}(e_1) + \mathrm{vr}(e_2) && \text{\# didn't remove/insert any variables} \\
&\leq 2^{h(e_1)} + 2^{h(e_2)} && \text{\# } H(\{e_1, e_2\}) \\
&\leq 2 \times 2^{\max(h(e_1), h(e_2))} && \text{\# } h(e_1), h(e_2) \leq \max \\
&= 2^{\max(h(e_1), h(e_2)) + 1} \\
&= 2^{h((e_1 \odot e_2))} && \text{\# defn of } h
\end{aligned}
$$

$P((e_1 \odot e_2))$, i.e. $P((e_1 \odot e_2))$

So $C(\{e_1, e_2\})$ follows

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

$\{\ldots, -4, -3, -2\}$ $\mathbb{Z}$ have PWO ~~$\{\ldots, 3, 4, \ldots\}$~~

$\mathbb{Q} - \{\frac{1}{n} : n \in \mathbb{N} - \{0\}\}$ $\mathbb{R} - (0, 1)$

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

$15 \div 6 \quad 2r3$

$15 = 2 \cdot 6 + 3$

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

$23, 6$

$23 = 3 \cdot 6 + 5$

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

not proved using well-ordering

...in order to have

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

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

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

Proof Using WO

Let $m, n \in \mathbb{N}$, $n > 0$.

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

R is not empty, since $m \in R$, since $m = 0 \cdot n + m$

Let r' be least element of R # exists by PWO

Let $q' \in \mathbb{N}$, $m = q'n + r'$ # by defn of r'

Must show $r' < n$.

Suppose not, ie suppose $r' \geq n$

Then $r' - n \geq 0$ # subtract n from $r' \geq n$

And $m = q'n + r' = (q'+1)n + r' - n$ # $q'n + r' = q'n + n + r' - n$

But then $r' - n \in R$ $\longrightarrow$ $\longleftarrow$ contradiction

So $r' < n$, since assuming otherwise leads to contradiction

$m = q'n + r' \wedge n > r'$, as claimed

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

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

$>$: beats.

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

$A > D$ $S > J$ $O > A$

$D > S$ $J > O$

$A > D > S > J > O > A$

Case $A > S$: 4-cycle

Case $S > A$

$A > D > S > A$ 3-cycle.

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

Proof - well-ordering principle.

~~Let~~

Claim: $\forall n \in \mathbb{N} - \{0,1,2\}, P(n)$. Let T be a tournament with n players and a cycle.

Let $C = \{c \in \mathbb{N} ; c$ is the length (# of players) in cycles in $T\}$

Let c' be the least element of C # C is non-empty by assumption

Suppose $c' > 3$.

Then there is some cycle $p_1 > p_2 > p_3 > \cdots > p_{c'}$

There are two cases to consider

Case $p_1 > p_3$ Then $p_1 > p_3 > \cdots > p_{c'}$ is a cycle of length $c'-1$ $\rightarrow\leftarrow$ c' is least element of C

Case $p_3 > p_1$ Then $p_1 > p_2 > p_3 > p_1$ is a cycle of length $3 < c'$ $\rightarrow\leftarrow$ since c' least element

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

$c' \not> 3$, since supposing that leads to a contradiction

$c' \leq 3$, but there are no cycles of length 1: $p_1 > p_1$!

or length 2: $p_1 > p_2 > p_1$

So $c' = 3$.

There is a 3-cycle.

Notes