Tutorial ex 3 up soon

CSC236 fall 2012

subtle 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, Section 1.2–1.3

Outline

Well-ordering

Higher, and more, base cases

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

Fundamental Theorem of Arithmetic
you can always find a quotient and remainder

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.

Read course notes approach for a comparison

Principle of well-ordering

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

$\{\frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$!

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?

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

subset of $\mathbb{N}$ and non-empty because $m \in R$, because $m = 0 \cdot n + m$

If so, we still need to be sure that

1. $0 \leq r < n$ ← use the fact that it is smallest
2. That q and r are unique — no other natural numbers would work — follow approach in Vassos's notes.

...in order to have

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

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

$\forall m \in \mathbb{N}, \forall n \in \mathbb{N} - \{0\}, \underbrace{\exists q, r \in \mathbb{N}, m = qn + r \wedge 0 \le r < n} =: P(m,n)$

Proof (using well ordering)

assume $m \in \mathbb{N}$ and $n \in \mathbb{N} - \{0\}$.
Let $R = \{r \in \mathbb{N} \mid \exists q \in \mathbb{N}, m = qn + r\}$. Note that $m \in R$, since $m = 0 \cdot n + m$. That means that R is a non-empty subset of $\mathbb{N}$, so it has a least element (by well-ordering). Let's call the least element r', so there must be a corresponding $q' \in \mathbb{N}$ st $m = q'n + r'$. It remains to show that $n > r' \geq 0$. Since r' is chosen from a subset of $\mathbb{N}$, we know $r' \geq 0$. Suppose $r' \geq n$. Then we would have $m = q'n + r' = q'n + r' - n + n = (q'+1)n + r' - n$, and $(q'+1), r' - n \in R$, contradicting r' being least element. So $n > r' \geq 0$.

So, $\forall m \in \mathbb{N}, n \in \mathbb{N} - \{0\}, \exists q, r \in \mathbb{N}, m = qn + r \wedge n > r \geq 0$.

It remains to show they are unique $\longrightarrow$

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

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

The question is to satisfy skeptics who say "maybe there are more choices, say $q'', r'' \in \mathbb{N}$ so that $m = q''n + r''$ and $n > r'' \geq 0$". The course notes show that, in this case $q' = q''$ and $r' = r''$. Basically you subtract equations:

$$m = q'n + r' = q''n + r'',$$

so

$(q' - q'')n = (r'' - r')$. If these are 0, we're done. Otherwise you have $|r'' - r'| \geq n$, but these numbers are in $[0, n-1]$, contradiction!

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

$P(n)$: $\underbrace{\text{Every round-robin tournament with } n \text{ players that has a cycle has a 3-cycle}}_{P(n)}$

no games for $n = 0, 1$
one game for $n = 2$, with one winner.

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

This notation for "beats" is not same as arithmetic $>$
– not transitive!

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

Consider game between P_1 and P_3

either $P_1 > P_3 \longrightarrow (n-1)$ cycle.

OR $P_3 > P_1 \longrightarrow 3$ cycle!

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

$P(n)$: $\underbrace{\text{Every round-robin tournament with } n \text{ players that has a cycle has a 3-cycle}}_{P(n).}$

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

Proof (well ordering)

assume $n \in \mathbb{N} - \{0,1,2\}$ and we have a tournament of n players with a cycle.

Let $C = \{c \in \mathbb{N} \mid \text{the tournament has a } c\text{-cycle}\}$.

Then, by assumption $|C| > 0$, since we assumed there is a cycle. So, by well-ordering, C has a least element; call it c'. Clearly $c' \geq 3$, since no cycles of length 0, 1, 2 are possible.

Suppose $c' > 3$, that is there is a cycle $p_1 > p_2 > p_3 > \dots > p_{c'} > p_1$. Then there are 2 cases:

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

Case 1 $\quad p_3 > p_1$. Then there is a 3-cycle,

$p_1 > p_2 > p_3 > p_1 \longrightarrow\longleftarrow$ contradiction

Case 2 $\quad p_1 > p_3$. Then there is a $(c'-1)$-cycle

$p_1 > p_3 > \ldots > p_{c'} > p_1 \longrightarrow\longleftarrow$ contradicting

c' being least element.

In both cases there is a contradiction, so $c' \leq 3$.

Thus $c' = 3$, and there is a 3-cycle.

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

$2^n > 10n$: $P(n)$

Where do we start?

$P(n)$ is false for $n < 6$.

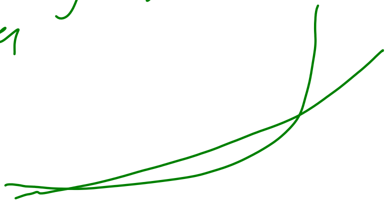
It's not true for several low values of n. You could re-write the predicate as $P'(n) : 2^{n+6} > 10(n+6)$, but why not just start later?

base case $n = 6$

$3^n \geq n^3$

Check your induction step

True for every n, but not every real number



Look at the graph.

The behaviour we use in the induction step is different for different parts of graph.

≈ 2.5

$3^n \geq n^3$

Check your induction step

Look at the graph.