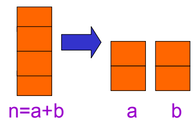
Mathematics for Computer Science
MIT 6.042J/18.062J

Induction II
Strong Induction
Well-order principle

Unstacking game



- Start: n boxes in one stack
- Move: pick any stack, divide into two nonempty stacks
- Scoring: if chosen stack is of size $a+b$ and you divide into two stacks of size a and b, you get ab points
- Overall score: total sum of scores for each move

Ordinary Induction

Ordinary induction allows proving $P(n+1)$ from $P(n)$ only

Why? Seems unfair, since started at 0, then showed
$0 \to 1,\ 1 \to 2,\ 2 \to 3, \ldots, n\text{-}1 \to n$.
So by the time we got to n+1,already know *all* of
$P(0), P(1), \ldots, P(n)$

Strong Induction

Allows proving $P(n+1)$ from *all* of
$P(0), P(1), \ldots, P(n)$,
instead of just $P(n)$.

Strong Induction

0 red and
(if everything $\leq n$ red then $n+1$ red)

then everything is red.

$$\frac{R(0),\ [\forall n\ [\forall\ k \leq n\ \ R(k)] \to R(n+1)]}{\forall m\ \ R(m)}$$

Strong vs. Ordinary Induction

MetaTheorem: Can transform any Strong Induction proof into Ordinary Induction.

Reprove by *ordinary* induction using induction hypothesis: $Q(n) ::= \ \forall k \leq n\ P(k)$

Earlier Strong Induction now goes through by Ordinary Induction.

Strong vs. Ordinary Induction

So why use Strong?

-- Convenience: no need to include $\forall k \le n$ all over.

Problems

Class Problem 1

Well-ordering Principle

Well-ordering principle

Every nonempty set of
nonnegative integers
has a
least element.

Familiar? Now you mention it, Yes.
Obvious? Yes.
Trivial? Yes. But watch out:

Well-ordering principle

Every nonempty set of
nonnegative ~~integers~~ rationals
has a
least element.

NO!

Well-ordering principle

Every nonempty set of
~~nonnegative~~ integers
has a
least element.

NO!

Proof using well-order principle

Theorem: $\sqrt{2}$ is irrational.
Proof (by contradiction):

- Suppose $\sqrt{2}$ was rational.
- Choose m, n integers without common prime factors (always possible) such that

$$\sqrt{2} = \frac{m}{n}$$

- Show that m & n are both even, a **contradiction**!

Proof using well-order principle

- Choose m, n integers without common prime factors (always possible)
- WHY IS IT ALWAYS POSSIBLE?

First: can assume $m \geq 0$

Next: by WOP, pick minimum m_0 such that $q=m_0/n_0$ for some n_0

If m_0 and n_0 had common factor p then could write $q=(m_0/p)/(n_0/p)$
Contradicts minimality of m_0!

Well-ordering principle

Theorem: Every integer > 1 is a product of primes.

Proof: (by contradiction) Suppose not.
Then set of nonproducts is nonempty.
By WOP, there is a least $n > 1$ that is not a product of primes.
In particular, n is not prime.

Well-ordering principle

Theorem: Every integer > 1 is a product of primes.

Proof: …So $n = k \cdot m$ for integers k, m where $n > k,m > 1$.
Since k,m smaller than the *least* nonproduct, both are prime products, *eg.,*

$$k = p_1 \cdot p_2 \cdots p_{94}$$
$$m = q_1 \cdot q_2 \cdots q_{214}$$

Well-ordering principle

Theorem: Every integer > 1 is a product of primes.

…So

$$n = k \cdot m = p_1 \cdot p_2 \cdots p_{94} \cdot q_1 \cdot q_2 \cdots q_{214}$$

is a prime product, a contradiction.
$\therefore$ The set of nonproducts > 1 must be empty. QED

Problems

Class Problem 2

