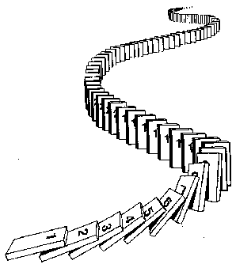
Foundations of Computer Science
Lecture 5

Induction: Proving "For All ..."

Induction: What and Why?
Induction: Good, Bad and Ugly
Induction, Well-Ordering and the Smallest Counter-Example



Last Time

1. Proving "IF ..., THEN ...".
2. Proving "... IF AND ONLY IF ...".
3. Proof patterns:
   - direct proof;
     - If $x, y \in \mathbb{Q}$, then $x + y \in \mathbb{Q}$.
     - If $4^x - 1$ is divisible by 3, then $4^{x+1} - 1$ is divisible by 3.
   - contraposition;
     - If r is irrational, then $\sqrt{r}$ is irrational.
     - If x^2 is even, then x is even.
   - contradiction.
     - $\sqrt{2}$ is irrational.
     - $a^2 - 4b \neq 2$.
     - $2\sqrt{n} + 1/\sqrt{n+1} \leq 2\sqrt{n+1}$.

Today: Induction, Proving "... for all ..."

1. What is induction.
2. Why do we need it?
3. The principle of induction. Toppling the dominos. The induction template.
4. Examples.
5. Induction, Well-Ordering and the Smallest Counter-Example.

Dispensing Postage Using 5¢ and 7¢ Stamps

19¢	20¢	21¢	22¢	23¢
7,7,5	5,5,5,5	7,7,7	5,5,5,7	?

Perseverance is a virtue when tinkering.

19¢	20¢	21¢	22¢	23¢	24¢	25¢	26¢	27¢	28¢
7,7,5	5,5,5,5	7,7,7	5,5,5,7	–	7,7,5,5	5,5,5,5,5	7,7,7,5	5,5,5,5,7	7,7,7,7

Can every postage greater than 23¢ can be dispensed?

Intuitively yes.

Induction formalizes that intuition.

Why Do We Need Induction?

	Predicate	Claim
(i)	$P(n) =$ "5¢ and 7¢ stamps can make postage n."	$\forall n \geq 24 : P(n)$
(ii)	$P(n) =$ "$n^2 - n + 41$ a prime number."	$\forall n \geq 1 : P(n)$
(iii)	$P(n) =$ "$4^n - 1$ is divisible by 3."	$\forall n \geq 1 : P(n)$

TINKER!

n	1	2	3	4	5	6	7	8	$\cdots$	40	41
$n^2 - n + 41$	41✓	43✓	47✓	53✓	61✓	71✓	83✓	97✓	$\cdots$	1601✓	1681✗
$(4^n - 1)/3$	1	5	21	85	341	1365	5461	21845	$\cdots$		

How can we prove something for *all* $n \geq 1$? Verification takes too long!

Prove for general n. Can be tricky.

Induction. Systematic.

Is $4^n - 1$ Divisible by 3 for $n \geq 1$?

$$P(n) = \text{"}4^n - 1 \text{ is divisible by 3."}$$

We proved:

$$\text{IF } \underbrace{4^n - 1 \text{ is divisible by 3}}_{P(n)}, \text{ THEN } \underbrace{4^{n+1} - 1 \text{ is divisible by 3}}_{P(n+1)}.$$

Proof. We prove the claim using a direct proof.

1: Assume that $P(n)$ is T, that is $4^n - 1$ is divisible by 3.
2: This means that $4^n - 1 = 3k$ for an integer k, or that $4^n = 3k + 1$.
3: Observe that $4^{n+1} = 4 \cdot 4^n$, and since $4^n = 3k + 1$, it follows that

$$4^{n+1} = 4 \cdot (3k + 1) = 12k + 4.$$

Therefore $4^{n+1} - 1 = 12k + 3 = 3(4k + 1)$ is a multiple of 3 ($4k + 1$ is an integer).
4: Since $4^{n+1} - 1$ is a multiple of 3, we have shown that $4^{n+1} - 1$ is divisible by 3.
5: Therefore, $P(n + 1)$ is T. ■

We proved:

$$P(n) \rightarrow P(n + 1)$$

What use is this? (Reasoning in the absense of facts.)

$4^n - 1$ is Divisible by 3 for $n \geq 1$

$$P(n) = \text{"}4^n - 1 \text{ is divisible by 3."}$$

$$P(n) \rightarrow P(n + 1)$$

NEW INFORMATION:

From tinkering we know that $P(1)$ is T: $4^1 - 3 = 3$ ← divisible by 3 (new fact)

$$\overset{\checkmark}{P(1)} \rightarrow \overset{\checkmark}{P(2)} \rightarrow \overset{\checkmark}{P(3)} \rightarrow \overset{\checkmark}{P(4)} \rightarrow \cdots \rightarrow \overset{\checkmark}{P(n-1)} \rightarrow \overset{\checkmark}{P(n)} \rightarrow \cdots$$

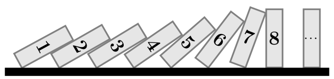
By Induction, $4^n - 1$ is Divisible by 3 for $n \geq 1$

$$P(n) = \text{"}4^n - 1 \text{ is divisible by 3."}$$

1. $P(1)$ is T.✓
2. $P(n) \rightarrow P(n + 1)$ is T.✓

} By induction, $P(n)$ is T for all $n \geq 1$.

$$\boxed{P(1)} \rightarrow P(2) \rightarrow P(3) \rightarrow P(4) \rightarrow P(5) \rightarrow \cdots$$



$P(n)$ form an infinite chain of dominos.
Topple the first and they *all* fall.

Practice. Exercise 5.2.

Induction Template

Induction to prove: $\forall n \geq 1 : P(n)$.

Proof. We use induction to prove $\forall n \geq 1 : P(n)$.

1: Show that $P(1)$ is T. ("simple" verification.) [base case]

2: Show $P(n) \to P(n+1)$ for $n \geq 1$ [induction step]

Prove *the implication* using direct proof or contraposition.

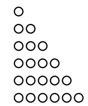
Direct	Contraposition
Assume $P(n)$ is T.	Assume $P(n+1)$ is F.
(valid derivations)	(valid derivations)
must show for any $n \geq 1$	must show for any $n \geq 1$
must use $P(n)$ here	must use $\neg P(n+1)$ here
Show $P(n+1)$ **is** T.	**Show** $P(n)$ **is** F.

3: Conclude: by induction, $\forall n \geq 1 : P(n)$. ■

- Prove the *implication* $P(n) \to P(n+1)$ for a *general* $n \geq 1$. (Often direct proof)
  Why is this easier than just proving $P(n)$ for general n?
- Assume $P(n)$ is T, and reformulate it mathematically.
- Somewhere in the proof you *must* use $P(n)$ to prove $P(n+1)$.
- End with a statement that $P(n+1)$ is T.

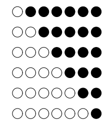
Sum of Integers

$$1 + 2 + 3 + \cdots + (n-1) + n \;=\; \textbf{?}$$



The GREAT Gauss (age 8-10):

$$\begin{array}{rcccccccc} S(n) &=& 1 &+& 2 &+& \cdots &+& n \\ S(n) &=& n &+& n-1 &+& \cdots &+& 1 \\ \hline 2S(n) &=& (n+1) &+& (n+1) &+& \cdots &+& (n+1) \\ &=& n \times (n+1) \end{array}$$



$$S(n) = 1 + 2 + 3 + \cdots + (n-1) + n = \tfrac{1}{2}n(n+1)$$

Proof: $\sum\limits_{i=1}^{n} i = \frac{1}{2}n(n+1)$

Proof. (By Induction) $P(n) : \sum\limits_{i=1}^{n} i = \frac{1}{2}n(n+1)$.

1: **[Base case]** $P(1)$ claims that $1 = \frac{1}{2} \times 1 \times (1+1)$, which is clearly T.

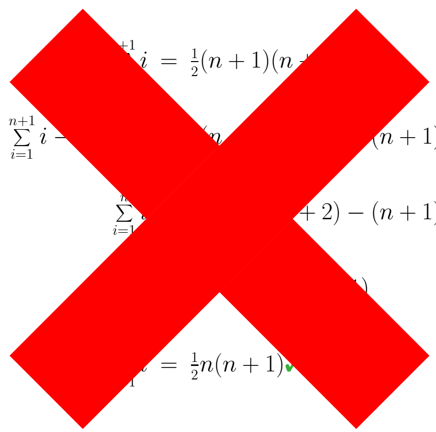
2: **[Induction step]** We show $P(n) \to P(n+1)$ for all $n \geq 1$, using a direct proof.
Assume (induction hypothesis) $P(n)$ *is* T*:* $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$.
Show $P(n+1)$ *is* T*:* $\sum_{i=1}^{n+1} i = \frac{1}{2}(\boldsymbol{n+1})(\boldsymbol{n+1}+1)$.

$$\begin{aligned} \sum_{i=1}^{n+1} i &= \sum_{i=1}^{n} \boldsymbol{i} + (n+1) && \text{[key step]} \\ &= \tfrac{1}{2}\boldsymbol{n(n+1)} + (n+1) && \text{[induction hypothesis } P(n)\text{]} \\ &= \tfrac{1}{2}(n+1)(n+2) && \text{[algebra]} \\ &= \tfrac{1}{2}(\boldsymbol{n+1})(\boldsymbol{n+1}+1). \end{aligned}$$

This is exactly what was to be shown. So, $P(n+1)$ is T.

3: By induction, $P(n)$ is T for all $n \geq 1$. ■

VERY BAD! Induction Step



Compare: $\sum\limits_{i=1}^{n+1} i = \sum\limits_{i=1}^{n} i + (n+1)$

(phew, nothing bad ☺)

$$\begin{array}{lrcll} & 7 &=& 4 & \\ \to & 4 &=& 7 & (a{=}b \to b{=}a) \\ \hline + & 11 &=& 11 ✓ & \text{(phew ☺)} \end{array}$$

(Have we proved 7=4?)

To start, you can **NEVER** assert (as though its true) what you are trying to prove.

Sum of Integer Squares

$$S(n) = 1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 + n^2 \;=\; \textbf{?}$$

Replace Gauss with TINKERING: *method of differences.*

	n	1	2	3	4	5	6	7
	$S(n)$	1	5	14	30	55	91	140
1st difference	$S'(n)$		4	9	16	25	36	49
2nd difference	$S''(n)$			5	7	9	11	13
3rd difference	$S'''(n)$				2	2	2	2

3'rd difference constant is like 3'rd derivative constant. So guess:

$$S(n) = a_0 + a_1 n + a_2 n^2 + a_3 n^3.$$

$$\begin{array}{ccccccccc} a_0 &+& a_1 &+& a_2 &+& a_3 &=& 1 \\ a_0 &+& 2a_1 &+& 4a_2 &+& 8a_3 &=& 5 \\ a_0 &+& 3a_1 &+& 9a_2 &+& 27a_3 &=& 14 \\ a_0 &+& 4a_1 &+& 16a_2 &+& 64a_3 &=& 30 \end{array}$$

$$a_0 = 0,\; a_1 = \tfrac{1}{6},\; a_2 = \tfrac{1}{2},\; a_3 = \tfrac{1}{3}$$

n	1	2	3	4	5	6	7	8	9	10
$\frac{1}{6}n + \frac{1}{2}n^2 + \frac{1}{3}n^3$	1	5	14	30	55	91	140	204	285	385

Proof: $S(n) = \sum_{i=1}^{n} i^2 = \frac{1}{6}n + \frac{1}{2}n^2 + \frac{1}{3}n^3 = \frac{1}{6}n(n+1)(2n+1)$

Proof. (By induction.) $P(n) : \sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

1: **[Base case]** $P(1)$, claims that $1 = \frac{1}{6} \times 1 \times 2 \times 3$, which is clearly T.

2: **[Induction step]** Show $P(n) \to P(n+1)$ for all $n \geq 1$. Direct proof.
Assume (induction hypothesis) $P(n)$ is T*:* $\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.
Show $P(n+1)$ is T*:* $\sum_{i=1}^{n+1} i^2 = \frac{1}{6}(n+1)(n+2)(2n+3)$.

$$\begin{aligned} \sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^{n} i^2 + (n+1)^2 && \text{[key step]} \\ &= \tfrac{1}{6}n(n+1)(2n+1) + (n+1)^2 && \text{[induction hypothesis } P(n)\text{]} \\ &= \tfrac{1}{6}(n+1)(n+2)(2n+3) && \text{[algebra]} \end{aligned}$$

This is exactly what was to be shown. So, $P(n+1)$ is T.

3: By induction, $P(n)$ is T for all $n \geq 1$. ■

Induction Gone Wrong

$$\boxed{\text{P}(1)} \to P(2) \to P(3) \to P(4) \to P(5) \to P(6) \to P(7) \to \cdots$$

No Base Case.

$$P(1) \to P(2) \to P(3) \to P(4) \to \cdots$$

False: $P(n) : n \leq n+1$ for all $n \geq 1$.

$$n \leq n+1 \to n+1 \leq n+2 \qquad \text{therefore} \qquad P(n) \to P(n+1).$$

[Every link is proved, but without the base case, you have *nothing*.]

Broken Chain.

$$\boxed{P(1)} \quad P(2) \to P(3) \to P(4) \to \cdots$$

False: $P(n)$: "all balls in any set of n balls are the same color."

Induction step. Suppose any set of n balls have the same color. Consider any set of $n+1$ balls $b_1, b_2, \ldots, b_n, b_{n+1}$. So, $b_1, b_2, \ldots, b_n$ have the same color and $b_2, b_3, \ldots, b_{n+1}$ have the same color. Thus $b_1, b_2, b_3, \ldots, b_{n+1}$ have the same color.

$$P(n) \to P(n+1)?$$

[A *single* broken link kills the entire proof.]

Well Ordering Principle

Well-ordering Principle.
Any non-empty set of natural numbers has a minimum element.

Induction follows from well ordering. Let $P(1)$ and $P(n) \to P(n+1)$ be T.

Suppose $P(n_*)$ fails for the **smallest** counter-example n_* (well-ordering).

$$\boxed{P(1)} \to \boxed{P(2)} \to \boxed{P(3)} \to \boxed{P(4)} \to \cdots \to \boxed{P(n_* - 1)} \to P(n_*) \to \cdots$$

Now how can $P(n_* - 1) \to P(n_*)$ be T?

Any induction proof can also be done using well-ordering.

Example Well-Ordering Proof: $n < 2^n$ for $n \geq 1$

Proof. [Induction] $P(n) : n < 2^n$.
Base case. $P(1)$ is T because $1 < 2^1$.
Induction. Assume $P(n)$ is T: $n < 2^n$. and show $P(n+1)$ is T: $n+1 < 2^{n+1}$.

$$n + 1 \leq n + n = 2n \leq 2 \times 2^n = 2^{n+1}.$$

Therefore $P(n+1)$ is T and, by induction, $P(n)$ is T for $n \geq 1$. ■

Proof. [Well-ordering] Proof by **contradiction**.
Assume that there is an $n \geq 1$ for which $n \geq 2^n$.
Let n_* be the **minimum** such **counter-example**, $n_* \geq 2^{n_*}$. ← well ordering
Since $1 < 2^1$, $n_* \geq 2$. Since $n_* \geq 2$, $\frac{1}{2}n_* \geq 1$ and so,

$$n_* - 1 \geq n_* - \tfrac{1}{2}n_* = \tfrac{1}{2}n_* \geq \tfrac{1}{2} \times 2^{n_*} = 2^{n_*-1}.$$

So, $n_* - 1$ is a *smaller* counter example. **FISHY!** ■

The **method of minimum counter-example** is very powerful.

Getting Good at Induction

TINKER

PRACTICE

Challenge. A circle has $2n$ distinct points, n are red and n are blue. Prove that one can start at a blue point and move clockwise always having passed as many blue points as red.

Practice. All exercises and pop-quizzes in chapter 5.
Strengthen. Problems in chapter 5.