Induction

Induction is perhaps the most important technique we'll learn for proving $\forall n P(n)$ when n ranges over the natural numbers.

- Later we'll see why it works for $\mathbb{N}$ and the extent to which it can be extended to other domains.

Induction

Induction is perhaps the most important technique we'll learn for proving $\forall n P(n)$ when n ranges over the natural numbers.

- Later we'll see why it works for $\mathbb{N}$ and the extent to which it can be extended to other domains.

Before going on, I want to make sure that you understand $P(n)$

- Suppose we want to prove that if n is odd, then so is n^2

Induction

Induction is perhaps the most important technique we'll learn for proving $\forall n P(n)$ when n ranges over the natural numbers.

- Later we'll see why it works for $\mathbb{N}$ and the extent to which it can be extended to other domains.

Before going on, I want to make sure that you understand $P(n)$

- Suppose we want to prove that if n is odd, then so is n^2

This statement has the form $\forall n P(n)$. What's $P(n)$?

Induction

Induction is perhaps the most important technique we'll learn for proving $\forall n P(n)$ when n ranges over the natural numbers.

- Later we'll see why it works for $\mathbb{N}$ and the extent to which it can be extended to other domains.

Before going on, I want to make sure that you understand $P(n)$

- Suppose we want to prove that if n is odd, then so is n^2

This statement has the form $\forall n P(n)$. What's $P(n)$?

- n is odd
- n^2 is odd
- if n is odd then so is n^2

Induction

Induction is perhaps the most important technique we'll learn for proving $\forall n P(n)$ when n ranges over the natural numbers.

- Later we'll see why it works for $\mathbb{N}$ and the extent to which it can be extended to other domains.

Before going on, I want to make sure that you understand $P(n)$

- Suppose we want to prove that if n is odd, then so is n^2

This statement has the form $\forall n P(n)$. What's $P(n)$?

- n is odd
- n^2 is odd
- if n is odd then so is n^2

What's $P(4)$?

- if 4 is odd, then so is 16

Induction

Induction is perhaps the most important technique we'll learn for proving $\forall n P(n)$ when n ranges over the natural numbers.

- Later we'll see why it works for $\mathbb{N}$ and the extent to which it can be extended to other domains.

Before going on, I want to make sure that you understand $P(n)$

- Suppose we want to prove that if n is odd, then so is n^2

This statement has the form $\forall n P(n)$. What's $P(n)$?

- n is odd
- n^2 is odd
- if n is odd then so is n^2

What's $P(4)$?

- if 4 is odd, then so is 16
- Note that $P(4)$ is true, because the antecedent is false.

Induction: The Basic Idea

Idea: To prove that a statement is true for all natural numbers, show that it is true for 1 (*base case* or *basis step*) and show that if it is true for n, it is also true for $n + 1$ (*inductive step*).

- The base case does not have to be 1; it could be 0, 2, 3, ...
- If the base case is k, then you are proving the statement for all $n \geq k$.

Induction: The Basic Idea

Idea: To prove that a statement is true for all natural numbers, show that it is true for 1 (*base case* or *basis step*) and show that if it is true for n, it is also true for $n+1$ (*inductive step*).

- The base case does not have to be 1; it could be 0, 2, 3, ...
- If the base case is k, then you are proving the statement for all $n \geq k$.

It is sometimes quite difficult to formulate the statement to prove.

IN THIS COURSE, WE WILL BE VERY FUSSY ABOUT THE FORMULATION OF THE STATEMENT TO PROVE. YOU MUST STATE IT VERY CLEARLY. WE WILL ALSO BE PICKY ABOUT THE FORM OF THE INDUCTIVE PROOF.

Writing Up a Proof by Induction

1. State the hypothesis very clearly:
   - Let $P(n)$ be the (English) statement . . . [some statement involving n]
2. The basis step
   - $P(k)$ holds because . . . [where k is the base case, usually 0 or 1]

Writing Up a Proof by Induction

1. State the hypothesis very clearly:
   - Let $P(n)$ be the (English) statement . . . [some statement involving n]
2. The basis step
   - $P(k)$ holds because . . . [where k is the base case, usually 0 or 1]
3. Inductive step
   - For all $n \geq k$, we prove that if $P(n)$ holds, then so does $P(n+1)$. That is, for all $n \geq k$, $P(n) \Rightarrow P(n+1)$.
4. Conclusion
   - Thus, we have shown by induction that $P(n)$ holds for all $n \geq k$ (where k was what you used for your basis step). [It's not necessary to always write the conclusion explicitly.]

A Simple Example

Theorem: For all positive integers n, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof: By induction. Let $P(n)$ be the statement

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Basis: $P(1)$ asserts that $\sum_{k=1}^{1} k = \frac{1(1+1)}{2}$. Since the LHS and RHS are both 1, this is true.

A Simple Example

Theorem: For all positive integers n, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof: By induction. Let $P(n)$ be the statement

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Basis: $P(1)$ asserts that $\sum_{k=1}^{1} k = \frac{1(1+1)}{2}$. Since the LHS and RHS are both 1, this is true.

Inductive step: Assume $P(n)$. We prove $P(n+1)$.
Note that $P(n+1)$ is the statement $\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$.

A Simple Example

Theorem: For all positive integers n, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof: By induction. Let $P(n)$ be the statement

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Basis: $P(1)$ asserts that $\sum_{k=1}^{1} k = \frac{1(1+1)}{2}$. Since the LHS and RHS are both 1, this is true.

Inductive step: Assume $P(n)$. We prove $P(n+1)$.
Note that $P(n+1)$ is the statement $\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$.

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \quad \text{[Induction hypothesis]} \\
&= \frac{n(n+1)+2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}$$

Thus, for all n, $P(n)$ implies $P(n+1)$, so $\forall n P(n)$ holds by induction.

Notes:

- You can write $\overset{P(n)}{=}$ instead of writing "Induction hypothesis" at the end of the line, or you can write "$P(n)$" at the of the line.
  - Whatever you write, make sure it's clear when you're applying the induction hypothesis
- Notice how we rewrite $\sum_{k=1}^{n+1} k$ so as to be able to appeal to the induction hypothesis. This is standard operating procedure.

Another example

Theorem: $(1+x)^n \geq 1+nx$ for all nonnegative integers n and all $x \geq -1$. (Take $0^0 = 1$.)

Proof: By induction on n. What's $P(n)$?

(a) $(1+x)^n \geq 1+nx$ for all $x \geq -1$.

(b) $(1+x)^n \geq 1+nx$ for all $n \geq 0$ and all $x \geq -1$.

Another example

Theorem: $(1+x)^n \geq 1+nx$ for all nonnegative integers n and all $x \geq -1$. (Take $0^0 = 1$.)

Proof: By induction on n. What's $P(n)$?

(a) $(1+x)^n \geq 1+nx$ for all $x \geq -1$.

(b) $(1+x)^n \geq 1+nx$ for all $n \geq 0$ and all $x \geq -1$.

It's (a). For the induction step, we will need to prove "for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$", but we don't want the "for all $n \geq 0$" to be part of $P(n)$. If it were, what would $P(0)$ be?

Another example

Theorem: $(1+x)^n \geq 1+nx$ for all nonnegative integers n and all $x \geq -1$. (Take $0^0 = 1$.)

Proof: By induction on n. What's $P(n)$?

(a) $(1+x)^n \geq 1+nx$ for all $x \geq -1$.

(b) $(1+x)^n \geq 1+nx$ for all $n \geq 0$ and all $x \geq -1$.

It's (a). For the induction step, we will need to prove "for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$", but we don't want the "for all $n \geq 0$" to be part of $P(n)$. If it were, what would $P(0)$ be?

Basis: $P(0)$ says $(1+x)^0 \geq 1$. This is clearly true for all $x \geq -1$.

Inductive Step: Assume $P(n)$. We prove $P(n+1)$.

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)^n(1+x) \\
&\geq (1+nx)(1+x) \quad \text{[Induction hypothesis]} \\
&= 1+nx+x+nx^2 \\
&= 1+(n+1)x+nx^2 \\
&\geq 1+(n+1)x
\end{aligned}$$

Inductive Step: Assume $P(n)$. We prove $P(n+1)$.

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n(1+x)\\ &\geq (1+nx)(1+x) \quad \text{[Induction hypothesis]}\\ &= 1+nx+x+nx^2\\ &= 1+(n+1)x+nx^2\\ &\geq 1+(n+1)x\end{aligned}$$

- Where did we use the assumption that $x \geq -1$?
  (a) We didn't use it; the statement is true for all x
  (b) We did

Why does induction work?

Suppose you've proved that $P(n)$ holds for all n by induction.

- So you've proved $P(1)$ and, for all n, $P(n)$ implies $P(n+1)$

If $P(n)$ doesn't hold for all n, there is a least natural number n^* for which it doesn't hold.

Why does induction work?

Suppose you've proved that $P(n)$ holds for all n by induction.

- So you've proved $P(1)$ and, for all n, $P(n)$ implies $P(n+1)$

If $P(n)$ doesn't hold for all n, there is a least natural number n^* for which it doesn't hold.

- This depends on the *Well Ordering Principle*: Every nonempty set of natural numbers has a smallest element.
  - Does the well ordering principle hold for the integers? the positive rational numbers? the positive real numbers?
- n^* can't be 1, because $P(1)$ holds by assumption.
- Can n^* be 2? Could it be 10?

Why does induction work?

Suppose you've proved that $P(n)$ holds for all n by induction.

- So you've proved $P(1)$ and, for all n, $P(n)$ implies $P(n+1)$

If $P(n)$ doesn't hold for all n, there is a least natural number n^* for which it doesn't hold.

- This depends on the *Well Ordering Principle*: Every nonempty set of natural numbers has a smallest element.
  - Does the well ordering principle hold for the integers? the positive rational numbers? the positive real numbers?
- n^* can't be 1, because $P(1)$ holds by assumption.
- Can n^* be 2? Could it be 10?

If n^* is the smallest integer for which $P(n^*)$ doesn't hold, and $n^* > 1$, then $P(n^* - 1)$ holds.

Why does induction work?

Suppose you've proved that $P(n)$ holds for all n by induction.

- So you've proved $P(1)$ and, for all n, $P(n)$ implies $P(n+1)$

If $P(n)$ doesn't hold for all n, there is a least natural number n^* for which it doesn't hold.

- This depends on the *Well Ordering Principle*: Every nonempty set of natural numbers has a smallest element.
  - Does the well ordering principle hold for the integers? the positive rational numbers? the positive real numbers?
- n^* can't be 1, because $P(1)$ holds by assumption.
- Can n^* be 2? Could it be 10?

If n^* is the smallest integer for which $P(n^*)$ doesn't hold, and $n^* > 1$, then $P(n^* - 1)$ holds.

- But we know that, for all n, if $P(n)$ holds, then $P(n+1)$ holds

Since $P(n^* - 1)$ holds, so does $P((n^* - 1) + 1)$.

But that means $P(n^*)$ holds, a contradiction!

Why does induction work?

Suppose you've proved that $P(n)$ holds for all n by induction.

- So you've proved $P(1)$ and, for all n, $P(n)$ implies $P(n+1)$

If $P(n)$ doesn't hold for all n, there is a least natural number n^* for which it doesn't hold.

- This depends on the *Well Ordering Principle*: Every nonempty set of natural numbers has a smallest element.
  - Does the well ordering principle hold for the integers? the positive rational numbers? the positive real numbers?
- n^* can't be 1, because $P(1)$ holds by assumption.
- Can n^* be 2? Could it be 10?

If n^* is the smallest integer for which $P(n^*)$ doesn't hold, and $n^* > 1$, then $P(n^* - 1)$ holds.

- But we know that, for all n, if $P(n)$ holds, then $P(n+1)$ holds

Since $P(n^* - 1)$ holds, so does $P((n^* - 1) + 1)$.

But that means $P(n^*)$ holds, a contradiction!

The Well Ordering Principle is essentially equivalent to induction.

- Both hold for the natural numbers

Another way of thinking about it

Suppose that P is a predicate on some domain D (where, D can be the natural numbers, but doesn't have to be). Suppose you can show

- $P(d_9)$, for some $d_0 \in D$
- for all $d \in D$, if $P(d)$ holds, then so do $P(f_1(d)), ..., P(f_m(d))$, where $f_1, \ldots, f_m$ are functions from D to D

Then what have you shown?

Another way of thinking about it

Suppose that P is a predicate on some domain D (where, D can be the natural numbers, but doesn't have to be). Suppose you can show

- $P(d_9)$, for some $d_0 \in D$
- for all $d \in D$, if $P(d)$ holds, then so do $P(f_1(d)), ..., P(f_m(d))$, where $f_1, \ldots, f_m$ are functions from D to D

Then what have you shown?

Define $R \subseteq D$ to be the smallest set of elements *reachable* from d by applying $f_1, \ldots, f_m$:

1. $d_0 \in R$
2. if $d' \in R$, then so are $f_1(d), \ldots, f_m(d)$ (i.e., R is *closed* under applications of $f_1, \ldots, f_m$)
3. and R is the smallest set that contains d and is closed under $f_1 \ldots, f_m$

Another way of thinking about it

Suppose that P is a predicate on some domain D (where, D can be the natural numbers, but doesn't have to be). Suppose you can show

- $P(d_9)$, for some $d_0 \in D$
- for all $d \in D$, if $P(d)$ holds, then so do $P(f_1(d)), ..., P(f_m(d))$, where $f_1, \ldots, f_m$ are functions from D to D

Then what have you shown?

Define $R \subseteq D$ to be the smallest set of elements *reachable* from d by applying $f_1, \ldots, f_m$:

1. $d_0 \in R$
2. if $d' \in R$, then so are $f_1(d), \ldots, f_m(d)$ (i.e., R is *closed* under applications of $f_1, \ldots, f_m$)
3. and R is the smallest set that contains d and is closed under $f_1 \ldots, f_m$
   - Why is there such a smallest set

Then all the elements in R satisfy P.

Induction is the special case where $f(n) = n + 1$.

Applying induction more broadly

Can we prove that $P(n)$ holds for all even n?

Applying induction more broadly

Can we prove that $P(n)$ holds for all even n?

- This is easy:
  - Base case: Prove $P(0)$
  - Inductive step: show that if $P(n)$ holds, then so does $P(n+2)$

The even number are exactly those reachable from 0 by applying the function $f(n) = n + 2$.

Applying induction more broadly

Can we prove that $P(n)$ holds for all even n?

- This is easy:
  - Base case: Prove $P(0)$
  - Inductive step: show that if $P(n)$ holds, then so does $P(n+2)$

The even number are exactly those reachable from 0 by applying the function $f(n) = n + 2$.

How about $P(n)$ for all integers?

Applying induction more broadly

Can we prove that $P(n)$ holds for all even n?

- This is easy:
  - Base case: Prove $P(0)$
  - Inductive step: show that if $P(n)$ holds, then so does $P(n+2)$

The even number are exactly those reachable from 0 by applying the function $f(n) = n + 2$.

How about $P(n)$ for all integers?

- Yes, with the right induction statement
  - Let $Q(n)$ (for $n \geq 0$) be the statement "Both $P(n)$ and $P(-n)$ hold". Now prove $Q(n)$ by induction for all $n \geq 0$. This gives us $P(n)$ for all integers.

Applying induction more broadly

Can we prove that $P(n)$ holds for all even n?

- This is easy:
  - Base case: Prove $P(0)$
  - Inductive step: show that if $P(n)$ holds, then so does $P(n+2)$

The even number are exactly those reachable from 0 by applying the function $f(n) = n + 2$.

How about $P(n)$ for all integers?

- Yes, with the right induction statement
  - Let $Q(n)$ (for $n \geq 0$) be the statement "Both $P(n)$ and $P(-n)$ hold". Now prove $Q(n)$ by induction for all $n \geq 0$. This gives us $P(n)$ for all integers.
- Alternatively, could prove that if $P(n)$ holds, then so do $P(n+1)$ and $P(n-1)$ (taking $f_1(n) = n + 1$ and $f_2(n) = n - 1$), but this could be harder!

How about $P(r)$ for all rational numbers r

- Can do this too:
  - Base case: Prove that $P(0/1)$ holds
  - Induction step: show, for all n and m, that if $P(n/m)$ holds, then so do $P(n+1/m)$ and $P(n/m+1)$.
- This will get the positive rationals; a little more work gets all the rationals.

All the positive rational number are reachable from $0/1$ using the $f_1(m/n) = (m+1)/n$ and $f_2(m/n) = m/(n+1)$.

How about $P(r)$ for all rational numbers r

- Can do this too:
  - Base case: Prove that $P(0/1)$ holds
  - Induction step: show, for all n and m, that if $P(n/m)$ holds, then so do $P(n+1/m)$ and $P(n/m+1)$.
- This will get the positive rationals; a little more work gets all the rationals.

All the positive rational number are reachable from $0/1$ using the $f_1(m/n) = (m+1)/n$ and $f_2(m/n) = m/(n+1)$.

How about $P(r)$ for all real numbers r?

- The set of elements reachable from a finite set of elements applying a finite set of functions is reachable, so we won't be able to cover the reals
- There is a notion of induction on the ordinals that can be applied.
  - The ordinals also satisfy the well-ordering principle.

We can also do induction on *trees*

- We want to show $\forall x P(x)$ is true, where x ranges over the nodes of the tree
- What's the base case?

We can also do induction on *trees*

- We want to show $\forall x P(x)$ is true, where x ranges over the nodes of the tree
- What's the base case?
  - Prove that $P(\text{root of tree})$ is true
- What's the inductive step?
  - Prove that if $P(x)$ is true, then $P(y)$ is true for all successors y of x on the tree.

We can also do induction on *trees*

- We want to show $\forall x P(x)$ is true, where x ranges over the nodes of the tree
- What's the base case?
  - Prove that $P(\text{root of tree})$ is true
- What's the inductive step?
  - Prove that if $P(x)$ is true, then $P(y)$ is true for all successors y of x on the tree.

We can also do induction on (propositional) formulas

- What's the base case?

We can also do induction on *trees*

- We want to show $\forall x P(x)$ is true, where x ranges over the nodes of the tree
- What's the base case?
  - Prove that P(root of tree) is true
- What's the inductive step?
  - Prove that if $P(x)$ is true, then $P(y)$ is true for all successors y of x on the tree.

We can also do induction on (propositional) formulas

- What's the base case?
  - Prove that P holds for all primitive propositions.

  What's the inductive step?

We can also do induction on *trees*

- We want to show $\forall x P(x)$ is true, where x ranges over the nodes of the tree
- What's the base case?
  - Prove that P(root of tree) is true
- What's the inductive step?
  - Prove that if $P(x)$ is true, then $P(y)$ is true for all successors y of x on the tree.

We can also do induction on (propositional) formulas

- What's the base case?
  - Prove that P holds for all primitive propositions.

  What's the inductive step?
  - If P holds for φ and ψ, it also holds for $\neg\varphi$ and $\varphi \wedge \psi$.

Towers of Hanoi

Problem: Move all the rings from pole 1 and pole 2, moving one ring at a time, and never having a larger ring on top of a smaller one.

How do we solve this?

- Think recursively!
- Suppose you could solve it for $n-1$ rings? How could you do it for n?

Towers of Hanoi

Problem: Move all the rings from pole 1 and pole 2, moving one ring at a time, and never having a larger ring on top of a smaller one.

How do we solve this?

- Think recursively!
- Suppose you could solve it for $n-1$ rings? How could you do it for n?

Solution

- Move top $n-1$ rings from pole 1 to pole 3 (we can do this by assumption)
  - Pretend largest ring isn't there at all
- Move largest ring from pole 1 to pole 2
- Move top $n-1$ rings from pole 3 to pole 2 (we can do this by assumption)
  - Again, pretend largest ring isn't there

This solution translates to a recursive algorithm:

- Suppose move($r \to s$) moves the top ring on pole r to pole s
- Note that if $r, s \in \{1, 2, 3\}$, then $6 - r - s$ is the other number in the set

procedure H(n, r, s) [Move n disks from r to s, $r \neq s$]
    if $n = 1$ **then** move($r \to s$)
        else $H(n - 1, r, 6 - r - s)$
            move($r \to s$)
            $H(n - 1, 6 - r - s, s)$
    endif
endproc

We can prove (by induction) that this algorithm does the right thing.

- What's the running time of the algorithm?
- How long does it take to move n rings from pole 1 to pole 2 according to this algorithm.

Towers of Hanoi: Analysis

Theorem: It takes $2^n - 1$ moves to perform $H(n, r, s)$, for all positive n, and all $r, s \in \{1, 2, 3\}$, $r \neq s$.

Proof: Let $P(n)$ be the statement "It takes $2^n - 1$ moves to perform $H(n, r, s)$ and all $r, s \in \{1, 2, 3\}$."

- Note that "for all positive n" is not part of $P(n)$!
- $P(n)$ is a statement about a particular n.
- If it were part of $P(n)$, what would $P(1)$ be?

Basis: $P(1)$ is immediate: move$(r \to s)$ is the only move in $H(1, r, s)$, and $2^1 - 1 = 1$.

Inductive step: Assume $P(n)$. To perform $H(n + 1, r, s)$, we first do $H(n, r, 6 - r - s)$, then move$(r \to s)$, then $H(n, 6 - r - s, s)$. Altogether, this takes $2^n - 1 + 1 + 2^n - 1 = 2^{n+1} - 1$ steps.

A Matching Lower Bound

Theorem: Any algorithm to move n rings from pole r to pole s requires at least $2^n - 1$ steps.

Proof: By induction, taking the statement of the theorem to be $P(n)$.

Basis: Easy: Clearly it requires (at least) 1 step to move 1 ring from pole r to pole s.

Inductive step: Assume $P(n)$. Suppose you have a sequence of steps to move $n+1$ rings from r to s. There's a first time and a last time you move ring $n+1$:

- Let k be the first time
- Let k' be the last time.
- Possibly $k = k'$ (if you only move ring $n+1$ once)

Suppose at step k, you move ring $n+1$ from pole r to pole s'.

- You can't assume that $s' = s$, although this is optimal.

Key point:

- The top n rings have to be on the third pole, $6 - r - s'$
- Otherwise, you couldn't move ring $n+1$ from r to s'.

By $P(n)$, it took at least $2^n - 1$ moves to get the top n rings to pole $6 - r - s'$.

At step k', the last time you moved ring $n+1$, suppose you moved it from pole r' to s (it has to end up at s).

- the other n rings must be on pole $6 - r' - s$.
- By $P(n)$, it takes at least $2^n - 1$ moves to get them to ring s (where they have to end up).

So, altogether, there are at least $2(2^n - 1) + 1 = 2^{n+1} - 1$ moves in your sequence:

- at least $2^n - 1$ moves before step k
- at least $2^n - 1$ moves after step k'
- step k itself.

Of course, if $k \neq k'$ (that is, if you move ring $n+1$ more than once) there are even more moves in your sequence.

Strong Induction

Sometimes when you're proving $P(n+1)$, you want to be able to use $P(j)$ for $j \leq n$, not just $P(n)$. You can do this with *strong induction*.

1. Let $P(n)$ be the statement . . . [some statement involving n]
2. The basis step
   - $P(k)$ holds because . . . [where k is the base case, usually 0 or 1]
3. Inductive step
   - Assume $P(k), \ldots, P(n)$ holds. We show $P(n+1)$ holds as follows . . .

Although strong induction looks stronger than induction, it's not. Anything you can do with strong induction, you can do with regular induction, by appropriately modifying the induction hypothesis.

Strong Induction

Sometimes when you're proving $P(n+1)$, you want to be able to use $P(j)$ for $j \leq n$, not just $P(n)$. You can do this with *strong induction*.

1. Let $P(n)$ be the statement . . . [some statement involving n]
2. The basis step
   - $P(k)$ holds because . . . [where k is the base case, usually 0 or 1]
3. Inductive step
   - Assume $P(k), \ldots, P(n)$ holds. We show $P(n+1)$ holds as follows . . .

Although strong induction looks stronger than induction, it's not. Anything you can do with strong induction, you can do with regular induction, by appropriately modifying the induction hypothesis.

- If $P(n)$ is the statement you're trying to prove by strong induction, let $P'(n)$ be the statement $P(1), \ldots, P(n)$ hold. Proving $P'(n)$ by regular induction is the same as proving $P(n)$ by strong induction.

An example using strong induction

Theorem: Any item costing $n > 7$ kopecks can be bought using only 3-kopeck and 5-kopeck coins.

Proof: Using strong induction. Let $P(n)$ be the statement that n kopecks can be paid using 3-kopeck and 5-kopeck coins. We prove $P(n)$ for all $n \geq 8$.

Basis: $P(8)$ is clearly true since $8 = 3 + 5$.

Inductive step: Assume $P(8), \ldots, P(n)$ is true. We want to show $P(n+1)$. If $n+1$ is 9 or 10, then it's easy to see that there's no problem ($P(9)$ is true since $9 = 3 + 3 + 3$, and $P(10)$ is true since $10 = 5 + 5$). Otherwise, note that $(n+1) - 3 = n - 2 \geq 8$. Thus, $P(n-2)$ is true, using the induction hypothesis. This means we can use 3- and 5-kopeck coins to pay for something costing $n-2$ kopecks. One more 3-kopeck coin pays for something costing $n+1$ kopecks.

An example using strong induction

Theorem: Any item costing $n > 7$ kopecks can be bought using only 3-kopeck and 5-kopeck coins.

Proof: Using strong induction. Let $P(n)$ be the statement that n kopecks can be paid using 3-kopeck and 5-kopeck coins. We prove $P(n)$ for all $n \geq 8$.

Basis: $P(8)$ is clearly true since $8 = 3 + 5$.

Inductive step: Assume $P(8), \ldots, P(n)$ is true. We want to show $P(n+1)$. If $n+1$ is 9 or 10, then it's easy to see that there's no problem ($P(9)$ is true since $9 = 3 + 3 + 3$, and $P(10)$ is true since $10 = 5 + 5$). Otherwise, note that $(n+1) - 3 = n - 2 \geq 8$. Thus, $P(n-2)$ is true, using the induction hypothesis. This means we can use 3- and 5-kopeck coins to pay for something costing $n-2$ kopecks. One more 3-kopeck coin pays for something costing $n+1$ kopecks.

How could you do this using regular induction?

Faulty Inductions

Part of why we want you to write out your assumptions carefully is so that you don't get led into some standard errors.

Theorem: All cats are black.

Faulty Inductions

Part of why we want you to write out your assumptions carefully is so that you don't get led into some standard errors.

Theorem: All cats are black.

Proof by induction: Let $P(n)$ be the statement: For any set of n cats, if at least one of them is a black, then all of them are.

Basis: Clearly OK.

Inductive step: Assume $P(n)$. Let's prove $P(n+1)$.

Given a set W of $n+1$ cats, one of which is black. Let A and B be two subsets of W of size n, each of which contains the known black cat, whose union is W.

By the induction hypothesis, each of A and B consists of all black cats. Thus, so does W. This proves $P(n) \Rightarrow P(n+1)$.

Take W to be the set of cats in the world, and let $n = |W|$. Since there is clearly at least one black cat in the world, it follows that all cats are black!

Where's the bug?

(a) There's no problem; the proof is correct.

(b) You're not allowed to use an induction hypothesis like "For any set of n cats, if at least one of them is a black, then all of them are."

(c) There's a problem in the base case.

(d) There's a problem in the induction step.

Theorem: Every integer $n > 1$ is a product of prime numbers.

Proof: By strong induction. Let $P(n)$ be the statement that n is a product of prime numbers.

Basis: $P(2)$ is clearly true.

Induction step: Assume $P(2), \ldots, P(n)$. We prove $P(n+1)$. If $n+1$ is prime, we are done. If not, it factors somehow. Suppose that $n+1 = rs$, for $r, s > 1$. By the induction hypothesis, r and s can be written as the product of primes. Thus, so can $n+1$.

But now how about

Theorem: Every integer $n > 1$ can be written as the a product of prime numbers in a unique way.

This result is also true. Let's try proving it by strong induction.

- Now $P(n)$ says that n can be written as the product of primes in a unique way.
- Base case $P(2)$ still holds.
- For the inductive step, if $n+1 = rs$, we can still assume that r and s can be written as the product of primes in a unique way.
- Does it follow that $n+1$ can be written as the product of primes in a unique way?

But now how about

Theorem: Every integer $n > 1$ can be written as the a product of prime numbers in a unique way.

This result is also true. Let's try proving it by strong induction.

- Now $P(n)$ says that n can be written as the product of primes in a unique way.
- Base case $P(2)$ still holds.
- For the inductive step, if $n+1 = rs$, we can still assume that r and s can be written as the product of primes in a unique way.
- Does it follow that $n+1$ can be written as the product of primes in a unique way?
  (a) Yes
  (b) No

Problem: Suppose $n + 1 = 36$. That is, you've proved that every number up to 36 has a unique factorization. Now you need to prove it for 36.

36 isn't prime, but $36 = 3 \times 12$. By the induction hypothesis, 12 has a unique prime factorization, say $p_1 p_2 p_3$. Thus, $36 = 3 p_1 p_2 p_3$.

However, 36 is also 4×9. By the induction hypothesis, $4 = q_1 q_2$ and $9 = r_1 r_2$. Thus, $36 = q_1 q_2 r_1 r_2$.

How do you know that $3 p_1 p_2 p_3 = q_1 q_2 r_1 r_2$.
(It does, but it doesn't follow from the induction hypothesis.)

This is a *breakdown error*. If you're trying to show something is unique, and you break it down (as we broke down $n + 1$ into r and s) you have to argue that nothing changes if we break it down a different way. What if $n + 1 = tu$?

- The actual proof of this result is quite subtle

Theorem: The sum of the internal angles of a regular n-gon is $180(n-2)$ for $n \geq 3$.

Proof: By induction. Let $P(n)$ be "the sum of the internal angles of a regular n-gon is $180(n-2)$." For $n = 3$, the result was shown in high school. Assume $P(n)$; let's prove $P(n+1)$. Given a regular $(n+1)$-gon, we can lop off one of the corners.

By the induction hypothesis, the sum of the internal angles of the regular n-gon is $180(n-2)$ degrees; the sum of the internal angles of the triangle is 180 degrees. Thus, the internal angles of the original $(n+1)$-gon is $180(n-1)$.
What's wrong??

Theorem: The sum of the internal angles of a regular n-gon is $180(n-2)$ for $n \geq 3$.

Proof: By induction. Let $P(n)$ be "the sum of the internal angles of a regular n-gon is $180(n-2)$." For $n = 3$, the result was shown in high school. Assume $P(n)$; let's prove $P(n+1)$. Given a regular $(n+1)$-gon, we can lop off one of the corners.

By the induction hypothesis, the sum of the internal angles of the regular n-gon is $180(n-2)$ degrees; the sum of the internal angles of the triangle is 180 degrees. Thus, the internal angles of the original $(n+1)$-gon is $180(n-1)$.
What's wrong??

- When you lop off a corner, you don't get a *regular* n-gon.

Theorem: The sum of the internal angles of a regular n-gon is $180(n-2)$ for $n \geq 3$.

Proof: By induction. Let $P(n)$ be "the sum of the internal angles of a regular n-gon is $180(n-2)$." For $n = 3$, the result was shown in high school. Assume $P(n)$; let's prove $P(n+1)$. Given a regular $(n+1)$-gon, we can lop off one of the corners.

By the induction hypothesis, the sum of the internal angles of the regular n-gon is $180(n-2)$ degrees; the sum of the internal angles of the triangle is 180 degrees. Thus, the internal angles of the original $(n+1)$-gon is $180(n-1)$.
What's wrong??

- When you lop off a corner, you don't get a *regular* n-gon.

The fix: **Strengthen the induction hypothesis**.

- Let $P(n)$ say that the sum of the internal angles of *any* n-gon is $180(n-2)$.

Inductive Definitions

Example: Define $\sum_{k=1}^{n} a_k$ inductively (i.e., by induction on n):

- $\sum_{k=1}^{1} a_k = a_1$
- $\sum_{k=1}^{n+1} a_k = \sum_{k=1}^{n} a_k + a_{n+1}$

The inductive definition avoids the use of $\cdots$, and thus is less ambiguous.

Example: An inductive definition of $n!$:

- $1! = 1$
- $(n+1)! = (n+1)n!$

Could even start with $0! = 1$.

An inductive definition of propositional formulas:

- Start with primitive propositions, close off under $\neg$ and $\wedge$
- More formally:
  - Let Φ_0 consist of all primitive propositions
  - Let $\Phi_{n+1} = \Phi_n \cup \{\neg\varphi, \varphi \wedge \psi : \varphi, \psi \in \Phi_n\}$.
  - $\Phi^* = \cup_{n=0}^{\infty} \Phi_n$ is the set of propositional formulas

An Inductive Definition of Transitive Closure

Given a relation R on S, here is a constructive inductive definition of transitive closure. Define $R_0, R_1, \ldots$ inductively:

- Let $R_0 = R$.
- Let $R_{n+1} = R_n \cup \{(s,t) : \exists u \in S((s,u) \in R_n, (u,t) \in R_n)\}$.
- Let $R' = \cup_{n=0}^{\infty} R_n$.

An Inductive Definition of Transitive Closure

Given a relation R on S, here is a constructive inductive definition of transitive closure. Define $R_0, R_1, \ldots$ inductively:

- Let $R_0 = R$.
- Let $R_{n+1} = R_n \cup \{(s,t) : \exists u \in S((s,u) \in R_n, (u,t) \in R_n)\}$.
- Let $R' = \cup_{n=0}^{\infty} R_n$.

Theorem: R' is the transitive closure of R.

What do you have to prove to show that this is true?

An Inductive Definition of Transitive Closure

Given a relation R on S, here is a constructive inductive definition of transitive closure. Define $R_0, R_1, \ldots$ inductively:

- Let $R_0 = R$.
- Let $R_{n+1} = R_n \cup \{(s,t) : \exists u \in S((s,u) \in R_n, (u,t) \in R_n)\}$.
- Let $R' = \cup_{n=0}^{\infty} R_n$.

Theorem: R' is the transitive closure of R.

What do you have to prove to show that this is true?

- $R \subseteq R'$

An Inductive Definition of Transitive Closure

Given a relation R on S, here is a constructive inductive definition of transitive closure. Define $R_0, R_1, \ldots$ inductively:

- Let $R_0 = R$.
- Let $R_{n+1} = R_n \cup \{(s,t) : \exists u \in S((s,u) \in R_n, (u,t) \in R_n)\}$.
- Let $R' = \cup_{n=0}^{\infty} R_n$.

Theorem: R' is the transitive closure of R.

What do you have to prove to show that this is true?

- $R \subseteq R'$
- R' is transitive
- If R'' is transitive and $R \subseteq R''$, then $R' \subseteq R''$ (i.e., R' is the smallest transitive set that contains R).

This will be homework.

Fibonacci Numbers

[Leonardo of Pisa, 12th century:] Suppose you start with two rabbits, one of each gender. After two months, they produce two rabbits (one of each gender) as offspring. Each subsequent pair of offspring behaves the same way, producing another pair in two months. Rabbits never die. How many rabbits do you have after n months?

Let f_n be the number of pairs after n months.
By assumption, $f_1 = f_2 = 1$
For $n > 2$, $f_{n+1} = f_n + f_{n-1}$

- In month $n+1$, each pair of rabbits that have been around for at least two months (f_{n-1}) produces another pair. So you have f_{n-1} new pairs on top of the f_n you had after n months.
- This is an *inductive definition* of a sequence

The Fibonacci sequence has the form 1, 1, 2, 3, 5, 8, ...

Fibonacci numbers grow exponentially

The Fibonacci sequence has lots of nice properties; we'll prove one.
Let $r = (1 + \sqrt{5})/2 \approx 1.62$.

Claim: $f_n \geq r^{n-2}$ for all n.

Where did this weird r come from?

- It's a solution to the equation $r^2 = r + 1$.
  - The other solution is $(1 - \sqrt{5})/2$, but that's negative

We can prove the claim by induction.
Base case: $f_1 = 1$; $r^{-1} = 1/r < 1$; so $f_1 > r^{-1}$
$f_2 = 1$; $r^0 = 1$; so $f_2 \geq r^0$.
Inductive step: If $n \geq 2$

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ &\geq r^{n-2} + r^{n-3} \\ &= r^{n-3}(r+1) \\ &= r^{n-3} r^2 && [\text{since } r + 1 = r^2] \\ &= r^{n-1} \end{aligned}$$

That's it!

The Sorites Paradox

If a pile of sand has $1,000,000$ grains of sand, it's a heap.
Removing one grain of sand from a heap leaves 1 heap.
Therefore, by induction, if a pile of sand has only one grain, it's also a heap.

Prove by induction on n that if a pile of sand has $1,000,000 - n$ grains of sand, it's a heap.

Where's the bug?

- This leads to a whole topic in the philosophy of language called "vagueness"

The Trust Game

Consider a game where, after n steps, there are piles of money on the table:

- The big one has $\$2^{n+1}$; the small one has $\$2^{n-1}$

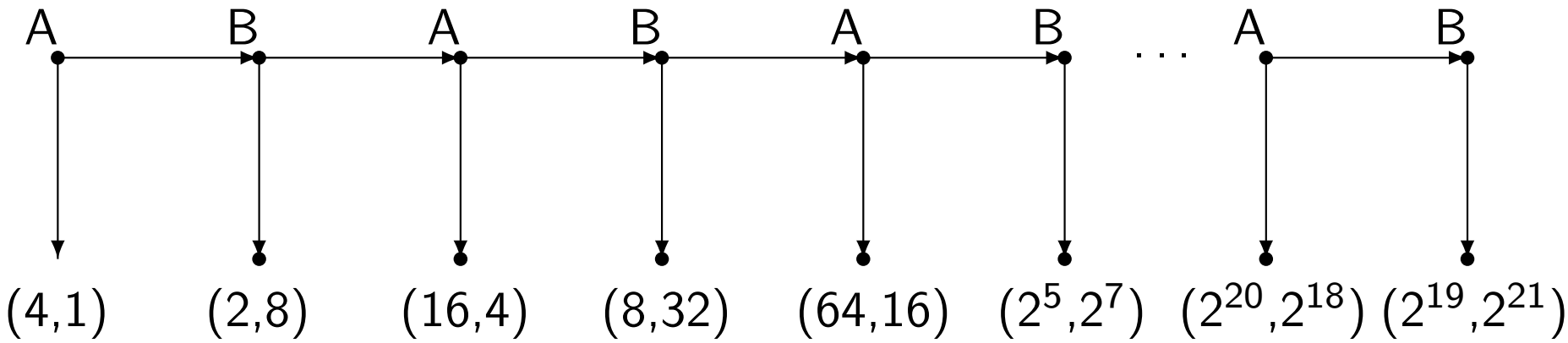
There are two players, Alice and Bob. Initially Alice is in charge. She can either quit the game or continue

- If she quits, she gets the money in the bigger pile ($4) and Bob gets the money in the smaller pile ($1)
- If she continues, Bob is in charge
- If he quits, he gets the money in the bigger pile ($8), Alice gets the money in the smaller pile ($2).
- If he continues, Alice is in charge, and so on.
- The game goes on for 20 steps;
  - if they're still playing then, Bob gets $\$2^{21}$ ($>$ \$2,000,000); Alice gets $\$2^{19}$ ($\approx$ \$500,000)

What should you do?

- Should you trust the other player to keep playing, or take your money and run?

In the game theory literature, this is called the *centipede game*.



What should Alice do if they're still playing at step 19?

- If she quits, she gets $\$2^{20}$ (about \$1,000,000); if she continues she gets only $\$2^{19}$).
- So Alice will quit, which means Bob will get $\$2^{18}$

So what should Bob do if they're still playing at step 18?

- If he quits, he gets $\$2^{19}$; if he continues, most likely he'll get $\$2^{18}$, since Alice will quit at step 19.
- So Bob quts, which means Alice will get $\$2^{16}$.

Continuing this way (by *backwards induction*), Alice quits at step 1 and gets \$4!

Under a specific model of *rationality*, quitting at the first step is the only right thing to do.

The muddy children puzzle

We can prove by induction on k that if k children have muddy foreheads, they say "yes" on the k^{th} question.
It appears as if the father didn't tell the children anything they didn't already know. Yet without the father's statement, they could not have deduced anything.
So what was the role of the father's statement?