Induction

This is perhaps the most important technique we'll learn for proving things.

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

This is perhaps the most important technique we'll learn for proving things.

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
   - Assume $P(n)$. We prove $P(n+1)$ holds as follows ... Thus, $P(n) \Rightarrow P(n+1)$.
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, $P(n)$ implies $P(n+1)$, so the result is true 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. Let $P(n)$ be the statement $(1+x)^n \geq 1+nx$ for 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. Let $P(n)$ be the statement $(1+x)^n \geq 1 + nx$ for all $x \geq -1$.

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 $P(n+1)$.

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

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. Let $P(n)$ be the statement $(1+x)^n \geq 1 + nx$ for all $x \geq -1$.

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 $P(n+1)$.

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

- Why does this argument fail if $x < -1$?

Why does induction work?

The text has the usual domino picture. Let's look at it a little more carefully.

Why does induction work?

The text has the usual domino picture. Let's look at it a little more carefully.

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.

- n^* can't be 1, because $P(1)$ holds by assumption.

Thus, $P(n^* - 1)$ holds.

Why does induction work?

The text has the usual domino picture. Let's look at it a little more carefully.

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.

- n^* can't be 1, because $P(1)$ holds by assumption.

Thus, $P(n^* - 1)$ 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!

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

When can we apply induction?

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 $P(n+2)$

When can we apply induction?

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 $P(n+2)$

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

When can we apply induction?

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 $P(n+2)$

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

- Yes, with the right induction statement.
  - Base case: Prove $P(0)$
  - Induction step: Prove (for all n) that if $P(n)$ holds, then so do $P(n+1)$ and $P(n-1)$.

When can we apply induction?

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 $P(n+2)$

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

- Yes, with the right induction statement.
  - Base case: Prove $P(0)$
  - Induction step: Prove (for all n) that if $P(n)$ holds, then so do $P(n+1)$ and $P(n-1)$.

How about $P(a/b)$ for all rational numbers a and b?

- 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.

When can we apply induction?

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 $P(n+2)$

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

- Yes, with the right induction statement.
  - Base case: Prove $P(0)$
  - Induction step: Prove (for all n) that if $P(n)$ holds, then so do $P(n+1)$ and $P(n-1)$.

How about $P(a/b)$ for all rational numbers a and b?

- 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.

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

- This is a lost cause

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($r \to s$) imoves 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 ≠ s]
    if n = 1 then move(r → s)
              else H(n − 1, r, 6 − r − s)
                   move(r → 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 runing 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.

Bubble Sort

Suppose we wanted to sort n items. Here's one way to do it:

Input n [number of items to be sorted]
$w_1, \ldots, w_n$ [items]

Algorithm BubbleSort
for $i = 1$ to $n - 1$
  for $j = 1$ to $n - i$
    if $w_j > w_{j+1}$ **then** switch(w_j, w_{j+1}) **endif**
  endfor
endfor

Why is this right:

- Intuitively, because largest elements "bubble up" to the top

How many comparisons?

- Best case, worst case, average case all the same:
  - $(n-1) + (n-2) + \cdots + 1 = n(n-1)/2$

Proving Bubble Sort Correct

We want to show that the algorithm is correct by induction. What's the statement of the induction?

Could take $P(n)$ to be the statement: the algorithm works correctly for n inputs.

- That turns out to be a tough induction statement to work with.
- Suppose $P(1)$ is true. How do you prove $P(2)$?

Proving Bubble Sort Correct

We want to show that the algorithm is correct by induction. What's the statement of the induction?

Could take $P(n)$ to be the statement: the algorithm works correctly for n inputs.

- That turns out to be a tough induction statement to work with.
- Suppose $P(1)$ is true. How do you prove $P(2)$?

A better choice:

- $P(k)$ is the statement that, if there are n inputs and $k \leq n-1$, then after k iterations of the outer loop, $w_{n-k+1}, \ldots, w_n$ are the k largest items, sorted in the right order.
  - Note that $P(k)$ is vacuously true if $k \geq n$.

Basis: How do we prove $P(1)$? By a nested induction!

This time, take $Q(l)$ to be the statement that, if $l \leq n-1$, then after l iterations of the inner loop, $w_{l+1} > w_j$, for $j = 1, \ldots, l$.

How to Guess What to Prove

Sometimes formulating $P(n)$ is straightforward; sometimes it's not. This is what to do:

- Compute the result in some specific cases
- Conjecture a generalization based on these cases
- Prove the correctness of your conjecture (by induction)

Example

Suppose $a_1 = 1$ and $a_n = a_{\lceil n/2 \rceil} + a_{\lfloor n/2 \rfloor}$ for $n > 1$. Find an explicit formula for a_n.

Try to see the pattern:

- $a_1 = 1$
- $a_2 = a_1 + a_1 = 1 + 1 = 2$
- $a_3 = a_2 + a_1 = 2 + 1 = 3$
- $a_4 = a_2 + a_2 = 2 + 2 = 4$

Suppose we modify the example. Now $a_1 = 3$ and $a_n = a_{\lceil n/2 \rceil} + a_{\lfloor n/2 \rfloor}$ for $n > 1$. What's the pattern?

- $a_1 = 3$
- $a_2 = a_1 + a_1 = 3 + 3 = 6$
- $a_3 = a_2 + a_1 = 6 + 3 = 9$
- $a_4 = a_2 + a_2 = 6 + 6 = 12$

$a_n = 3n$!

Theorem: If $a_1 = k$ and $a_n = a_{\lceil n/2 \rceil} + a_{\lfloor n/2 \rfloor}$ for $n > 1$, then $a_n = kn$ for $n \geq 1$.

Proof: By strong induction. Let $P(n)$ be the statement that $a_n = kn$.

Basis: $P(1)$ says that $a_1 = k$, which is true by hypothesis.

Inductive step: Assume $P(1), \ldots, P(n)$; prove $P(n+1)$.

$$\begin{aligned} a_{n+1} &= a_{\lceil (n+1)/2 \rceil} + a_{\lfloor (n+1)/2 \rfloor} \\ &= k\lceil (n+1)/2 \rceil + k\lfloor (n+1)/2 \rfloor \quad \text{[Induction hypothesis]} \\ &= k(\lceil (n+1)/2 \rceil + \lfloor (n+1)/2 \rfloor) \\ &= k(n+1) \end{aligned}$$

Theorem: If $a_1 = k$ and $a_n = a_{\lceil n/2 \rceil} + a_{\lfloor n/2 \rfloor}$ for $n > 1$, then $a_n = kn$ for $n \geq 1$.

Proof: By strong induction. Let $P(n)$ be the statement that $a_n = kn$.

Basis: $P(1)$ says that $a_1 = k$, which is true by hypothesis.

Inductive step: Assume $P(1), \ldots, P(n)$; prove $P(n+1)$.

$$\begin{aligned} a_{n+1} &= a_{\lceil (n+1)/2 \rceil} + a_{\lfloor (n+1)/2 \rfloor} \\ &= k\lceil (n+1)/2 \rceil + k\lfloor (n+1)/2 \rfloor \quad \text{[Induction hypothesis]} \\ &= k(\lceil (n+1)/2 \rceil + \lfloor (n+1)/2 \rfloor) \\ &= k(n+1) \end{aligned}$$

We used the fact that $\lceil n/2 \rceil + \lfloor n/2 \rfloor = n$ for all n (in particular, for $n+1$). To see this, consider two cases: n is odd and n is even.

- if n is even, $\lceil n/2 \rceil + \lfloor n/2 \rfloor = n/2 + n/2 = n$
- if n is odd, suppose $n = 2k+1$
  - $\lceil n/2 \rceil + \lfloor n/2 \rfloor = (k+1) + k = 2k+1 = n$

Theorem: If $a_1 = k$ and $a_n = a_{\lceil n/2 \rceil} + a_{\lfloor n/2 \rfloor}$ for $n > 1$, then $a_n = kn$ for $n \geq 1$.

Proof: By strong induction. Let $P(n)$ be the statement that $a_n = kn$.

Basis: $P(1)$ says that $a_1 = k$, which is true by hypothesis.

Inductive step: Assume $P(1), \ldots, P(n)$; prove $P(n+1)$.

$$\begin{aligned} a_{n+1} &= a_{\lceil (n+1)/2 \rceil} + a_{\lfloor (n+1)/2 \rfloor} \\ &= k\lceil (n+1)/2 \rceil + k\lfloor (n+1)/2 \rfloor \quad \text{[Induction hypothesis]} \\ &= k(\lceil (n+1)/2 \rceil + \lfloor (n+1)/2 \rfloor) \\ &= k(n+1) \end{aligned}$$

We used the fact that $\lceil n/2 \rceil + \lfloor n/2 \rfloor = n$ for all n (in particular, for $n+1$). To see this, consider two cases: n is odd and n is even.

- if n is even, $\lceil n/2 \rceil + \lfloor n/2 \rfloor = n/2 + n/2 = n$
- if n is odd, suppose $n = 2k+1$
  - $\lceil n/2 \rceil + \lfloor n/2 \rfloor = (k+1) + k = 2k+1 = n$

This proof has a (small) gap:

- We should check that $\lceil (n+1)/2 \rceil \leq n$

One more example

Find a formula for

$$\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\frac{1}{7\cdot 10}+\cdots+\frac{1}{(3n-2)(3n+1)}$$

Some values:

- $r_1 = 1/4$
- $r_2 = 1/4 + 1/28 = 8/28 = 2/7$
- $r_3 = 1/4+1/28+1/70 = (70+10+4)/280 = 84/280 = 3/10$

Can you see the pattern?

One more example

Find a formula for

$$\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\frac{1}{7\cdot 10}+\cdots+\frac{1}{(3n-2)(3n+1)}$$

Some values:

- $r_1 = 1/4$
- $r_2 = 1/4 + 1/28 = 8/28 = 2/7$
- $r_3 = 1/4+1/28+1/70 = (70+10+4)/280 = 84/280 = 3/10$

Can you see the pattern?

Conjecture: $r_n = n/(3n+1)$. Let this be $P(n)$.

Basis: $P(1)$ says that $r_1 = 1/4$.

Inductive step:

$$\begin{aligned} r_{n+1} &= r_n + \tfrac{1}{(3n+1)(3n+4)} \\ &= \tfrac{n}{3n+1} + \tfrac{1}{(3n+1)(3n+4)} \\ &= \tfrac{n(3n+4)+1}{(3n+1)(3n+4)} \\ &= \tfrac{3n^2+4n+1}{(3n+1)(3n+4)} \\ &= \tfrac{(n+1)(3n+1)}{(3n+1)(3n+4)} = \tfrac{n+1}{3n+4} \end{aligned}$$

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 women are blondes.

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 women are blondes.

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

Basis: Clearly OK.

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

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

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

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

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 women are blondes.

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

Basis: Clearly OK.

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

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

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

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

Where's the bug?

Theorem: Every integer > 1 has a unique prime factorization.

[The result is true, but the following proof is not:]

Proof: By strong induction. Let $P(n)$ be the statement that n has a unique factorization. We prove $P(n)$ for $n > 1$.

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 $n+1 = rs$ $r, s > 1$. By the induction hypothesis, r has a unique factorization $\Pi_i p_i$ and s has a unique prime factorization $\Pi_j q_j$. Thus, $\Pi_i p_i \Pi_j q_j$ is a prime factorization of $n+1$, and since none of the factors of either piece can be changed, it must be unique.

What's the flaw??

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, $36 = 3p_1 p_2 p_3$.

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 $3p_1 p_2 p_3 = q_1 q_2 r_1 r_2$.
(They do, 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??

- 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 $180(n-2)$.

Consider 0-1 sequences in which 1's may not appear consecutively, except in the rightmost two positions.

- 010110 is not allowed, but 010011 is

Prove that there are 2^n allowed sequences of length n for $n \geq 1$

Why can't this be right?

Consider 0-1 sequences in which 1's may not appear consecutively, except in the rightmost two positions.

- 010110 is not allowed, but 010011 is

Prove that there are 2^n allowed sequences of length n for $n \geq 1$

Why can't this be right?

"Proof" Let $P(n)$ be the statement of the theorem.

Basis: There are 2 sequences of length 1—0 and 1—and they're both allowed.

Inductive step: Assume $P(n)$. Let's prove $P(n+1)$. Take any allowed sequence x of length n. We get a sequence of length $n+1$ by appending either a 0 or 1 at the end. In either case, it's allowed.

- If x ends with a 1, it's OK, because $x1$ is allowed to end with 2 1's.

Thus, $s_{n+1} = 2s_n = 22^n = 2^{n+1}$.

Where's the flaw?

Consider 0-1 sequences in which 1's may not appear consecutively, except in the rightmost two positions.

- 010110 is not allowed, but 010011 is

Prove that there are 2^n allowed sequences of length n for $n \geq 1$

Why can't this be right?

"Proof" Let $P(n)$ be the statement of the theorem.

Basis: There are 2 sequences of length 1—0 and 1—and they're both allowed.

Inductive step: Assume $P(n)$. Let's prove $P(n+1)$. Take any allowed sequence x of length n. We get a sequence of length $n+1$ by appending either a 0 or 1 at the end. In either case, it's allowed.

- If x ends with a 1, it's OK, because $x1$ is allowed to end with 2 1's.

Thus, $s_{n+1} = 2s_n = 22^n = 2^{n+1}$.

Where's the flaw?

- What if x already ends with 2 1's?

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 $0! = 1$.

Inductive Definitions of Sets

A *palindrome* is an expression that reads the same backwards and forwards:

- Madam I'm Adam
- Able was I ere I saw Elba

What is the set of palindromes over $\{a, b, c, d\}$? Two approaches:

1. The smallest set P such that
   (a) P contains a, b, c, d, aa, bb, cc, dd
   (b) if x is in P, then so is axa, bxb, cxc, and dxd

   Things to think about:
   - How do you know that there is a smallest set (one which is a subset of all others)
   - How do you know that it doesn't contain ab
2. Define P_n, the palindromes of length n, inductively:
   - $P_1 = \{a, b, c, d\}$
   - $P_2 = \{aa, bb, cc, dd\}$
   - $P_{n+1} = \{axa, bxb, cxc, dxd | x \in P_{n-1}\}$ for $n \geq 2$

   Let $P' = \cup_n P_n$.

Theorem: $P = P'$. (The two approaches define the same set.)
Proof: Show $P \subseteq P'$ and $P' \subseteq P$.
To see that $P \subseteq P'$, it suffices to show that

(a) P' contains a, b, c, d, aa, bb, cc, dd

(b) if x is in P', then so is axa, bxb, cxc, and dxd

(since P is the smallest set with these properties).

Clearly $P_1 \cup P_2$ satisfies (1), so P' does. And if $x \in P'$, then $x \in P_n$ for some n, in which case axa, bxb, cxc, and dxd are all in P_{n+2} and hence in P'. Thus, $P \subseteq P'$.

To see that $P' \subseteq P$, we prove by strong induction that $P_n \subseteq P$ for all n. Let $P(n)$ be the statement "$P_n \subseteq P$."

Basis: $P_1, P_2 \subseteq P$: Obvious.

Suppose $P_1, \ldots, P_n \subseteq P$. If $n \geq 2$, the fact that $P_{n+1} \subseteq P$ follows immediately from (b). (Actually, all we need is the fact that $P_{n-1} \subseteq P$, which follows from the (strong) induction hypothesis.)

Thus, $P' = \cup_n P_n \subseteq P$.

Recall that the set of palindromes is the smallest set P such that

(a) P contains a, b, c, d, aa, bb, cc, dd

(b) if x is in P, then so is axa, bxb, cxc, and dxd

"Smallest" is not in terms of cardinality.

- P is guaranteed to be infinite

"Smallest" is in terms of the subset relation.

Here's a set that satisfies (a) and (b) and isn't the smallest:

Define Q_n inductively:

- $Q_1 = \{a, b, c, d\}$
- $Q_2 = \{aa, bb, cc, dd, ab\}$
- $Q_{n+1} = \{axa, bxb, cxc, dxd | x \in Q_{n-1}\}$, $n \geq 2$

Let $Q = \cup_n Q_n$.

It's easy to see that Q satisfies (a) and (b), but it isn't the smallest set to do so.

Fibonacci Numbers

[Leonardi 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 $(1 - \sqrt{5})/2$

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 $n \geq 2$

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

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 $\$2^{n-1}$

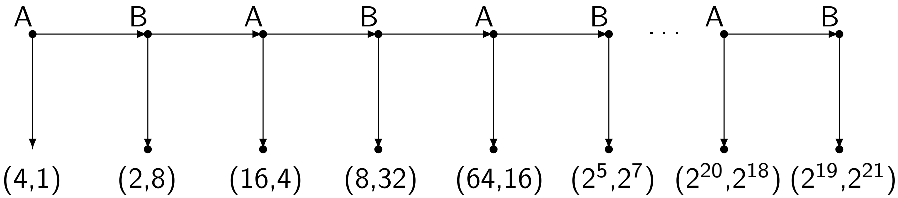
There are two players, Alice and Bob. Initially Alice is in charge. She can either quit the game or continue

- 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?