Methods of Proof

One way of proving things is by induction.

• That’s coming next.

What if you can’t use induction?

Typically you’re trying to prove a statement like “Given $X$, prove (or show that) $Y$”. This means you have to prove $X \Rightarrow Y$

In the proof, you’re allowed to assume $X$, and then show that $Y$ is true, using $X$.

• A special case: if there is no $X$, you just have to prove $Y$ or $\text{true} \Rightarrow Y$.

Alternatively, you can do a proof by contradiction: Assume that $Y$ is false, and show that $X$ is false.

• This amounts to proving $\neg Y \Rightarrow \neg X$

Example

Theorem $n$ is odd iff (in and only if) $n^2$ is odd, for $n \in \mathbb{Z}$.

Proof: We have to show

1. $n$ odd $\Rightarrow n^2$ odd
2. $n^2$ odd $\Rightarrow n$ odd

For (1), if $n$ is odd, it is of the form $2k + 1$. Hence,

$$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Thus, $n^2$ is odd.

For (2), we proceed by contradiction. Suppose $n^2$ is odd and $n$ is even. Then $n = 2k$ for some $k$, and $n^2 = 4k^2$. Thus, $n^2$ is even. This is a contradiction. Thus, $n$ must be odd.

A Proof By Contradiction

Theorem: $\sqrt{2}$ is irrational.

Proof: By contradiction. Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$ for some $a, b \in \mathbb{N}^+$. We can assume that $a/b$ is in lowest terms.

• Therefore, $a$ and $b$ can’t both be even.

Squaring both sides, we get

$$2 = a^2/b^2$$

Thus, $a^2 = 2b^2$, so $a^2$ is even. This means that $a$ must be even.

Suppose $a = 2c$. Then $a^2 = 4c^2$.

Thus, $4c^2 = 2b^2$, so $b^2 = 2c^2$. This means that $b^2$ is even, and hence so is $b$.

Contradiction!

Thus, $\sqrt{2}$ must be irrational.

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, I WILL BE VERY FUSSY ABOUT THE FORMULATION OF THE STATEMENT TO PROVE. YOU MUST STATE IT VERY CLEARLY. I WILL ALSO BE PICKY ABOUT THE FORM OF THE INDUCTION 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]

3. Inductive step
   • Assume $P(n)$. We prove $P(n + 1)$ holds as follows ... Thus, $P(n) \implies P(n + 1)$.

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.]

Notes:

• You can write $P(n)$ instead of writing “Induction hypothesis” at the end of the line, or you can write ”$P(n)$” at the end 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.

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

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

Thus, $P(n)$ implies $P(n + 1)$, so the result is true by induction.

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 $(1+x)^n \geq 1 + nx$.

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

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

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

• Why does this argument fail if $x < -1$?
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 robot\((r \rightarrow s)\) is a command to a robot to move 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 \( s \)\}

```plaintext
if \( n = 1 \) then
  robot\((r \rightarrow s)\)
else
  \( H(n - 1, r, 6 - r - s) \)
  robot\((r \rightarrow s)\)
  \( H(n - 1, 6 - r - s, s) \)
endif
return
endpro
```

**Towers of Hanoi: Analysis**

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

**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: robot\((r \rightarrow s)\) 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 robot\((r \rightarrow s)\), 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.

If 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 also 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, for $n \geq 8$.

**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:
  $o(n - 1) + (n - 2) + \cdots + 1 = n(n - 1)/2$
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 $P(2)$?

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 $j = 1, \ldots, l$.

Basis: $Q(1)$ holds because after the first iteration of the inner loop, $w_2 > w_1$ (thanks to the switch statement).

$Q(n-k-1)$ says that, after the $(k+1)$st iteration of the inner loop, $w_{n-k} > w_j$ for $j = 1, \ldots, k$. $P(k)$ says that the top $k$ elements are $w_{n-k+1}, \ldots, w_n$, in that order. Thus, the top $k+1$ elements must be $w_{n-k}, \ldots, w_n$, in that order. This proves $P(k+1)$.

Note that $P(n-1)$ says that after $n-1$ iterations of the outer loop (which is all there are), the top $n-1$ elements are $w_2, \ldots, w_n$. So $w_1$ has to be the smallest element, and $w_1, w_2, \ldots, w_n$ is a sorted list.

Inductive step: Suppose that $Q(l)$ is true. If $l+1 \geq n-1$, then $Q(l+1)$ is vacuously true. If $l+1 < n$, by $Q(l)$, we know that $w_{l+1} > w_j$, for $j = 1, \ldots, l$ after $l$ iterations. The $(l+1)$st iteration of the inner loop compares $w_{l+1}$ and $w_{l+2}$. After the $(l+1)$st iteration, the bigger one is $w_{l+2}$. Thus, $w_{l+2} > w_{l+1}$. By the induction hypothesis, $w_{l+2} > w_j$, for $j = 1, \ldots, l$.

That completes the nested induction. Thus, $Q(l)$ holds for all $l$. $Q(n-1)$ says that $w_n > w_j$, for $j = 1, \ldots, n-1$. That’s just what $P(1)$ says. So we’re done with the base case of the main induction.

[Note: For a really careful proof, we need better notation (for value of $w_l$ before and after the switch).]

Inductive step (for main induction): Assume $P(k)$. Thus, $w_{k+1}, \ldots, w_n$ are the $k$ largest items. To prove $P(k+1)$, we use nested induction again:

- Now $Q(l)$ says “if $i = k+1$, then if $l \leq n - (k+1)$, after $l$ iterations of the inner loop, $w_{l+1} > w_j$, for $j = 1, \ldots, l$.”
- Almost the same as before, except that instead of saying “if $l \leq n - 1$,” we say “if $l \leq n - (k+1)$.”

  - If $i = k+1$, we go through the inner loop only $n - (k+1)$ times.

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?

- \( a_1 = 3 \)
- \( a_2 = a_1 + a_1 = 3 + 3 = 6 \)
- \( a_3 = a_2 + a_1 = 6 + 3 = 9 \)
- \( a_4 = a_2 + a_2 = 6 + 6 = 12 \)

\( a_n = 3n! \).