Strong Induction

me once i see that I have to prove something for all $n \in \mathbb{N}$
Announcements

- HW4 due Friday at 11:59 pm
  - There are 2 submission spots on Gradescope:
    Feedback before the midterm is only guaranteed if you don’t use late days

- Midterm this Monday in class

- Homework 5 releases on Monday
Midterm

• The reference sheets will be provided
• One practice midterm and solutions are posted
• Optional review session this Saturday, July 20th at 11:00am
Strong Induction
Let’s Try Another Induction Proof

**Fundamental Theorem of Arithmetic**

Every positive integer greater than 1 has a unique prime factorization.

Uniqueness is hard. Let’s just show existence.

I.e.

Claim: Every positive integer greater than 1 can be written as a product of primes.
Prime Factorizations

Some examples

\[ 12 = 2^2 \cdot 3 \]
\[ 35 = 5 \cdot 7 \]
\[ 36 = 2^2 \cdot 3^2 \]
\[ 7 = 7 \]

Notice, for prime numbers the product is just the one number.
Induction on Primes.

Let $P(n)$ be “$n$ can be written as a product of primes.”

We show $P(n)$ for all integers $n \geq 2$ by induction on $n$.

**Base Case ($n = 2$):** $2$ is a product of just itself. Since $2$ is prime, it is written as a product of primes.

**Inductive Hypothesis:**

**Inductive Step:**
Case 1, $k + 1$ is prime:
Case 2, $k + 1$ is composite:

Therefore $P(k + 1)$.

$P(n)$ holds for all $n \geq 2$ by the principle of induction.
Induction on Primes.

Let $P(n)$ be “$n$ can be written as a product of primes.”
We show $P(n)$ for all integers $n \geq 2$ by induction on $n$.

**Base Case ($n = 2$):** 2 is a product of just itself. Since 2 is prime, it is written as a product of primes.

**Inductive Hypothesis:** Suppose $P(k)$ holds for an arbitrary integer $k \geq 2$.

**Inductive Step:**
Case 1, $k + 1$ is prime: then $k + 1$ is automatically written as a product of primes.
Case 2, $k + 1$ is composite:

Therefore $P(k + 1)$.

$P(n)$ holds for all $n \geq 2$ by the principle of induction.
We’re Stuck

We can divide $k + 1$ up into smaller pieces (say $s, t$ such that $st = k + 1$ with $2 \leq s < k + 1$ and $2 \leq t < k + 1$

Is $P(s)$ true? Is $P(t)$ true?

I mean...it would be...

But in the inductive step we don’t have it...

Let’s add it to our inductive hypothesis.
Recall: Induction

Induction relied on the fact that:

\[ \forall n \, P(n) \equiv P(0) \land \forall k \, (P(k) \rightarrow P(k + 1)) \]

- **Base Case**: Prove \( P(0) \) holds.
- **Inductive Hypothesis**: Let \( k \geq 0 \) be an arbitrary integer. Suppose \( P(k) \) holds.
- **Inductive Step**: Prove that \( P(k + 1) \) holds (using \( P(k) \)).
Recall: Induction

Check that the formula holds for $n = 0$

Assume the formula holds for $n = k$.

Show that the assumption implies that the formula holds for $n = k + 1$.

Conclude that the formula holds for all $n \in \mathbb{N}$. 
Another Equivalence

There are other statements that are stronger but still useful to $\forall n \, P(n)$. In particular:

$$\forall n \, P(n) \equiv P(0) \land P(1) \land P(2) \land P(3) \ldots$$

$$\equiv P(0) \land (P(0) \rightarrow P(1)) \land ((P(0) \land P(1)) \rightarrow P(2)) \land$$

$$((P(0) \land P(1) \land P(2)) \rightarrow P(3)) \ldots$$

$$\equiv P(0) \land \forall k \, ((P(0) \land \cdots \land P(k)) \rightarrow P(k + 1))$$
The Principle of Strong Induction

\[ P(0) \land \forall k \left( (P(0) \land \cdots \land P(k)) \rightarrow P(k + 1) \right) \]

**Base Case**
Prove \( P(0) \) holds.

**Inductive Hypothesis**
Let \( k \geq 0 \) be an arbitrary integer. Suppose \( P(0) \land \cdots \land P(k) \) hold.

**Inductive Step**
Prove that \( P(k + 1) \) holds.
Strong Induction

That hypothesis where we assume $P(\text{base case}), \ldots, P(k)$ instead of just $P(k)$ is called a strong inductive hypothesis.

Strong induction is the same fundamental idea as weak (“regular”) induction.

$P(0)$ is true.
And $P(0) \rightarrow P(1)$, so $P(1)$.
And $P(1) \rightarrow P(2)$, so $P(2)$.
And $P(2) \rightarrow P(3)$, so $P(3)$.
And $P(3) \rightarrow P(4)$, so $P(4)$.

...
Strong Induction

Induction:  \( k \Rightarrow k + 1 \)

Strong Induction:  \( 0..k \Rightarrow k + 1 \)
Induction on Primes

Let $P(n)$ be “$n$ can be written as a product of primes.”
We show $P(n)$ for all integers $n \geq 2$ by induction on $n$.

**Base Case ($n = 2$):** 2 is a product of just itself. Since 2 is prime, it is written as a product of primes.

**Inductive Hypothesis:**

**Inductive Step:**
- Case 1, $k + 1$ is prime: then $k + 1$ is automatically written as a product of primes.
- Case 2, $k + 1$ is composite:

Therefore $P(k + 1)$.

$P(n)$ holds for all $n \geq 2$ by the principle of induction.
Induction on Primes

Let \( P(n) \) be "\( n \) can be written as a product of primes."

We show \( P(n) \) for all integers \( n \geq 2 \) by induction on \( n \).

**Base Case (\( n = 2 \)):** 2 is a product of just itself. Since 2 is prime, it is written as a product of primes.

**Inductive Hypothesis:** Suppose \( P(2), \ldots, P(k) \) hold for an arbitrary integer \( k \geq 2 \).

**Inductive Step:**

Case 1, \( k + 1 \) is prime: then \( k + 1 \) is automatically written as a product of primes.

Case 2, \( k + 1 \) is composite: We can write \( k + 1 = st \) for \( s, t \) nontrivial divisors (i.e. \( 2 \leq s < k + 1 \) and \( 2 \leq t < k + 1 \)). By inductive hypothesis, we can write \( s \) as a product of primes \( p_1 \cdots p_j \) and \( t \) as a product of primes \( q_1 \cdots q_\ell \). Multiplying these representations, \( k + 1 = p_1 \cdots p_j \cdot q_1 \cdots q_\ell \), which is a product of primes.

Therefore \( P(k + 1) \).

\( P(n) \) holds for all \( n \geq 2 \) by the principle of induction.
Strong Induction vs. Weak Induction

• “Normal” Induction is otherwise known as Weak Induction
• All induction proofs could be written by Strong Induction instead. It’s a *stronger* hypothesis to use. There is more to work with.
• However, there’s often the philosophy to only use a stronger hypothesis when needed to make your inductive step more clear.
Making Induction Proofs Pretty

All of our strong induction proofs will come in 5 easy(?) steps!

1. Define $P(n)$. State that your proof is by induction on $n$.

2. Base Case: Show $P(b)$ i.e. show the base case

3. Inductive Hypothesis: Suppose $P(b) \land \cdots \land P(k)$ for an arbitrary $k \geq b$.

4. Inductive Step: Show $P(k + 1)$ (i.e. get $[P(b) \land \cdots \land P(k)] \rightarrow P(k + 1)$)

5. Conclude by saying $P(n)$ is true for all $n \geq b$ by the principle of induction.
Practical Advice

How many base cases do you need?

• Always at least one.
• If you’re analyzing recursive code or a recursive function, at least one for each base case of the code/function.
• If you always go back $s$ steps, at least $s$ consecutive base cases.
• Enough to make sure every case is handled.
Strong Induction Example

Stamp Collection
Stamp Collection

• I have a collection of 4¢ and 5¢ stamps. Prove that for all \( n \geq 12 \), I can make \( n¢ \) worth of stamps.

• Examples:
  • \( 13¢ = 5¢ + 4¢ + 4¢ \)
  • \( 22¢ = 5¢ + 5¢ + 4¢ + 4¢ + 4¢ \)
[Attempted Proof by Strong Induction]
Prove that for all $n \geq 12$, I can make $n \$$ worth of stamps.

1. Let $P(n)$ be “I can make $n \$$ worth of stamps with just 4\$ and 5\$ stamps.” We prove $P(n)$ for all integers $n \geq 12$ by strong induction.

2. Base Case: 12\$ can be made with three 4\$ stamps. Thus $P(12)$ is true.

3. IH: Suppose $P(12) \land \cdots \land P(k)$ hold for an arbitrary integer $k \geq 12$. I.e. we can make $12\$$, $13\$$, ..., $k\$$ worth of stamps with just 4\$ and 5\$ stamps.

4. IS:

5. Conclusion: Thus $P(n)$ holds for all integers $n \geq 12$ by strong induction.
[Attempted Proof by Strong Induction]

Prove that for all $n \geq 12$, I can make $n \cent$ worth of stamps.

1. Let $P(n)$ be “I can make $n \cent$ worth of stamps with just 4\cent and 5\cent stamps.” We prove $P(n)$ for all integers $n \geq 12$ by strong induction.

2. Base Case: 12\cent can be made with three 4\cent stamps. Thus $P(12)$ is true.

3. IH: Suppose $P(12) \land \cdots \land P(k)$ hold for an arbitrary integer $k \geq 12$. I.e. we can make $12\cent, 13\cent, \ldots, k\cent$ worth of stamps with just 4\cent and 5\cent stamps.

4. IS: We aim to show $P(k + 1)$, i.e. that we can make $k + 1$ cents in stamps. By the IH, we can make $k - 3$ cents in stamps. Adding another 4\cent stamp gives exactly $k + 1$ cents.

5. Conclusion: Thus $P(n)$ holds for all integers $n \geq 12$ by strong induction.
What was the problem?

- We don’t know \( P(13) \) holds.

- When \( k = 12, \) and \( k + 1 = 13: \)
  - Our IH assumes just \( P(12) \)
  - In the IS, we say since \( P(9) \) holds (going back to \( k - 3 \)), then \( P(13) \) holds.
  - But we don’t know anything about \( P(9)! \) It might not even be true!

- Lesson: If we go back \( s \) steps in the IS, we need \( s \) base cases.
Tower Visualization

**BAD**
- P(17)
- P(16)
- P(15)
- P(14)
- P(13)
- **P(12)**

**GOOD**
- P(17)
- P(16)
- P(15)
- P(14)
- P(13)

base cases
[Proof by Strong Induction]
Prove that for all \( n \geq 12 \), I can make \( n \)¢ worth of stamps.

1. Let \( P(n) \) be “I can make \( n \)¢ worth of stamps with just 4¢ and 5¢ stamps.” We prove \( P(n) \) for all integers \( n \geq 12 \) by strong induction.

2. Base Cases:
   - 12¢ can be made with three 4¢ stamps. Thus \( P(12) \) is true.
   - 13¢ can be made with two 4¢ stamps and one 5¢ stamps. Thus \( P(13) \) is true.
   - 14¢ can be made with one 4¢ stamp and two 5¢ stamps. Thus \( P(14) \) is true.
   - 15¢ can be made with three 5¢ stamps. Thus \( P(15) \) is true.

3. IH: Suppose \( P(12) \land \cdots \land P(k) \) hold for an arbitrary integer \( k \geq 15 \). I.e. we can make 12¢, 13¢, ..., \( k \)¢ worth of stamps with just 4¢ and 5¢ stamps.

4. IS: We aim to show \( P(k + 1) \), i.e. that we can make \( k + 1 \) cents in stamps. By the IH, we can make \( k - 3 \) cents in stamps. Adding another 4¢ stamp gives exactly \( k + 1 \) cents.
   [Note: Now \( k + 1 \geq 16 \), so \( k - 3 \geq 12 \). We’re in the clear!]

5. Conclusion: Thus \( P(n) \) holds for all integers \( n \geq 12 \) by strong induction.
Strong Induction Lesson

"With great power comes great responsibility."
Ben Parker

Be careful about base cases!!
Strong Induction Template
Strong Induction Template

1. Define $P(n)$. State that your proof is by strong induction on $n$.
2. Base Case: Show your base cases $P(b_{\text{min}})$, ..., $P(b_{\text{max}})$ are true.
3. Inductive Hypothesis: Suppose $P(b_{\text{min}}) \land \cdots \land P(k)$ hold for an arbitrary integer $k \geq b_{\text{max}}$.
4. Inductive Step: Prove $P(k + 1)$ using the IH.
5. Conclusion: Conclude by saying $P(n)$ holds for all integers $n \geq b_{\text{min}}$ by strong induction.
Practical Tip

- If you aren’t sure how many steps you’ll go back, leave space for the base cases.
- Do the IH / IS, and then fill in the base cases later.
Strong Induction Example

Fibonacci Sequence
Fibonacci Numbers

• The Fibonacci Numbers are defined as follows:

\[ f_0 = 0 \]
\[ f_1 = 1 \]
\[ f_n = f_{n-1} + f_{n-2} \quad \text{for all } n \geq 2 \]

• i.e. 0, 1, 1, 2, 3, 5, 8, ...
Fibonacci Numbers Claim

• We claim that $f_n < 2^n$ for all $n \geq 0$.

- $f_0 = 0$  
  $2^0 = 1$
- $f_1 = 1$  
  $2^1 = 2$
- $f_2 = 1$  
  $2^2 = 4$
- $f_3 = 2$  
  $2^3 = 8$
- $f_4 = 3$  
  $2^4 = 16$

• We prove by strong induction!
Prove that for all $n \in \mathbb{N}$, $f_n < 2^n$.

1. Let $P(n)$ be

Definition:

$f_0 = 0, f_1 = 1$

$f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$
Prove that for all \( n \in \mathbb{N}, f_n < 2^n \).

1. Let \( P(n) \) be "\( f_n < 2^n \)". We prove \( P(n) \) for all \( n \in \mathbb{N} \) by strong induction.
2. Base Cases:

Definition:
\[
\begin{align*}
f_0 &= 0, f_1 = 1 \\
f_n &= f_{n-1} + f_{n-2} \quad \text{for } n \geq 2
\end{align*}
\]
Prove that for all $n \in \mathbb{N}$, $f_n < 2^n$.

1. Let $P(n)$ be "$f_n < 2^n$" We prove $P(n)$ for all $n \in \mathbb{N}$ by strong induction.

2. Base Cases:
   - $f_0 = 0$ and $2^0 = 1$. Since $0 < 1$, $P(0)$ holds.
   - $f_1 = 1$ and $2^1 = 2$. Since $1 < 2$, $P(1)$ holds.

3. IH:
Prove that for all $n \in \mathbb{N}$, $f_n < 2^n$.

1. Let $P(n)$ be "$f_n < 2^n$". We prove $P(n)$ for all $n \in \mathbb{N}$ by strong induction.

2. Base Cases:
   - $f_0 = 0$ and $2^0 = 1$. Since $0 < 1$, $P(0)$ holds.
   - $f_1 = 1$ and $2^1 = 2$. Since $1 < 2$, $P(1)$ holds.

3. IH: Suppose $P(0) \land \cdots \land P(k)$ hold for an arbitrary integer $k \geq 1$.

4. IS:

Definition:
- $f_0 = 0, f_1 = 1$
- $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$
Prove that for all $n \in \mathbb{N}$, $f_n < 2^n$.

1. Let $P(n)$ be "$f_n < 2^n$". We prove $P(n)$ for all $n \in \mathbb{N}$ by strong induction.
2. Base Cases:
   - $f_0 = 0$ and $2^0 = 1$. Since $0 < 1$, $P(0)$ holds.
   - $f_1 = 1$ and $2^1 = 2$. Since $1 < 2$, $P(1)$ holds.
3. IH: Suppose $P(0) \land \cdots \land P(k)$ hold for an arbitrary integer $k \geq 1$.
4. IS: We aim to show $P(k + 1)$, i.e. that $f_{k+1} < 2^{k+1}$.

**Definition:**

- $f_0 = 0$, $f_1 = 1$
- $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$
Prove that for all $n \in \mathbb{N}$, $f_n < 2^n$.

1. Let $P(n)$ be "$f_n < 2^n$" We prove $P(n)$ for all $n \in \mathbb{N}$ by strong induction.

2. Base Cases:
   - $f_0 = 0$ and $2^0 = 1$. Since $0 < 1$, $P(0)$ holds.
   - $f_1 = 1$ and $2^1 = 2$. Since $1 < 2$, $P(1)$ holds.

3. IH: Suppose $P(0) \land \cdots \land P(k)$ hold for an arbitrary integer $k \geq 1$.

4. IS: We aim to show $P(k + 1)$, i.e. that $f_{k+1} < 2^{k+1}$. Observe:
   \[
   f_{k+1} = f_k + f_{k-1} \quad \text{Since } k + 1 \geq 2 \\
   \leq 2^k + f_{k-1} \quad \text{By IH, since } P(k) \text{ is assumed} \\
   \leq 2^k + 2^{k-1} \quad \text{By IH, since } P(k - 1) \text{ is assumed} \\
   \leq 2^k + 2^k \quad \text{Since } 2^{k-1} = \frac{1}{2} \cdot 2^k \leq 2^k \\
   = 2^{k+1}
   \]

Definition:

$f_0 = 0, f_1 = 1$
$f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$
Prove that for all $n \in \mathbb{N}$, $f_n < 2^n$.

1. Let $P(n)$ be "$f_n < 2^n$" We prove $P(n)$ for all $n \in \mathbb{N}$ by strong induction.

2. Base Cases:
   - $f_0 = 0$ and $2^0 = 1$. Since $0 < 1$, $P(0)$ holds.
   - $f_1 = 1$ and $2^1 = 2$. Since $1 < 2$, $P(1)$ holds.

3. IH: Suppose $P(0) \land \cdots \land P(k)$ hold for an arbitrary integer $k \geq 1$.

4. IS: We aim to show $P(k + 1)$, i.e. that $f_{k+1} < 2^{k+1}$. Observe:
   \[
   f_{k+1} = f_k + f_{k-1} \quad \text{Since } k + 1 \geq 2 \\
   \leq 2^k + f_{k-1} \quad \text{By IH, since } P(k) \text{ is assumed} \\
   \leq 2^k + 2^{k-1} \quad \text{By IH, since } P(k - 1) \text{ is assumed} \\
   \leq 2^k + 2^k \quad \text{Since } 2^{k-1} = \frac{1}{2} \cdot 2^k \leq 2^k \\
   = 2^{k+1}
   \]

5. Conclusion: Thus $P(n)$ holds for all $n \in \mathbb{N}$ by strong induction.
Fibonacci Tower

\[
\begin{align*}
P(4) \quad & \quad P(3) \\
P(3) \quad & \quad P(2) \\
P(2) \quad & \quad P(1) \\
P(1) \quad & \quad P(0)
\end{align*}
\]

base cases
How many base cases?

• Always at least one base case.

• If you’re analyze a recursive function, at least one for each base case of the function.

• If you go back $s$ steps in the proof, at least $s$ base cases.
Prove that for all $n \in \mathbb{N}$, $f_n < 2^n$.

1. Let $P(n)$ be
2. Base Cases:
3. IH:
4. IS:
5. Conclusion:

Definition:
$f_0 = 0, f_1 = 1$
$f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$