Introduction to Mathematical Induction

- Many mathematical theorems assert that a property holds for all natural numbers, odd positive integers, etc.
- Mathematical induction: very important proof technique for proving such universally quantified statements
- Induction will come up over and over again in other classes: algorithms, programming languages, automata theory, etc.

Analogy

- Suppose we have an infinite ladder, and we know two things:
  1. We can reach the first rung of the ladder
  2. If we reach a particular rung, then we can also reach the next rung
- From these two facts, can we conclude we can reach every step of the infinite ladder?
- Answer is yes, and mathematical induction allows us to make arguments like this

Mathematical Induction

- Used to prove statements of the form \( \forall x \in \mathbb{Z}^+ \cdot P(x) \)
- An inductive proof has two steps:
  1. Base case: Prove that \( P(1) \) is true
  2. Inductive step: Prove \( \forall n \in \mathbb{Z}^+ \cdot P(n) \rightarrow P(n+1) \)
- Induction says if you can prove (1) and (2), you can conclude: \( \forall x \in \mathbb{Z}^+ \cdot P(x) \)

Example 1

- Prove the following statement by induction:
  \[ \forall n \in \mathbb{Z}^+. \sum_{i=1}^{n} i = \frac{(n)(n+1)}{2} \]
- Base case: \( n = 1 \). In this case, \( \sum_{i=1}^{1} i = 1 \) and \( \frac{(1)(1+1)}{2} = 1 \); thus, the base case holds.
- Inductive step: By the inductive hypothesis, we assume \( P(k) \):
  \[ \sum_{i=1}^{k} i = \frac{k(k+1)}{2} \]
  Now, we want to show \( P(k+1) \):
  \[ \sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2} \]
Example 1, cont.

- First, observe:
  \[ \sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) \]

- By the inductive hypothesis, \( \sum_{i=1}^{k} i = \frac{k(k+1)}{2} \); thus:
  \[ \sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + (k+1) \]

- Rewrite left hand side as:
  \[ \sum_{i=1}^{k+1} i = \frac{k^2 + 3k + 2}{2} = \frac{(k+1)(k+2)}{2} \]

- Since we proved both base case and inductive step, property holds.

Example 2

- Prove the following statement for all non-negative integers \( n \):
  \[ \sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \]

- Since need to show for all \( n \geq 0 \), base case is \( P(0) \), not \( P(1) \)!

- Base case (\( n = 0 \)): \( 2^0 = 1 = 2^1 - 1 \)

- Inductive step:
  \[ \sum_{i=0}^{k+1} 2^i = \sum_{i=0}^{k} 2^i + 2^{k+1} \]

Example 3

- Prove that \( 2^n < n! \) for all integers \( n \geq 4 \)

- Easy to make subtle errors when trying to prove things by induction – pay attention to details!

- Consider the statement: All horses have the same color

- What is wrong with the following \textit{bogus proof} of this statement?

- \( P(n) \): A collection of \( n \) horses have the same color

- Base case: \( P(1) \) ✓

Example 4

- Prove that \( 3 \mid (n^3 - n) \) for all positive integers \( n \).
**Bogus Proof, cont.**

- **Induction:** Assume $P(k)$; prove $P(k + 1)$
- Consider a collection of $k + 1$ horses: $h_1, h_2, \ldots, h_{k+1}$
- By IH, $h_1, h_2, \ldots, h_k$ have the same color; let this color be $c$
- By IH, $h_2, \ldots, h_{k+1}$ have same color; call this color $c'$
- Since $h_2$ has color $c$ and $c'$, we have $c = c'$
- Thus, $h_3, h_2, \ldots, h_{k+1}$ also have same color
- What’s the fallacy?

**Strong Induction**

- Slight variation on the inductive proof technique is **strong induction**
- Regular and strong induction only differ in the inductive step
  - **Regular induction:** assume $P(k)$ holds and prove $P(k + 1)$
  - **Strong induction:** assume $P(1), P(2), \ldots, P(k)$; prove $P(k + 1)$
- Strong induction can be viewed as standard induction with strengthened inductive hypothesis!

**Example, cont.**

- Let’s use a stronger predicate:
  
  $$Q(n) = \sum_{i=1}^{n} 2i - 1 = n^2$$

  - Clearly $Q(n) \rightarrow P(n)$
  - Now, prove $\forall n \in \mathbb{Z}+. Q(n)$ using induction!

**Motivation for Strong Induction**

- Prove that if $n$ is an integer greater than $1$, then it is either a prime or can be written as the product of primes.
- Let’s first try to prove the property using regular induction.
  - **Base case ($n=2$):** Since $2$ is a prime number, $P(2)$ holds.
  - **Inductive step:** Assume $k$ is either a prime or the product of primes.
  - But this doesn’t really help us prove the property about $k + 1$
  - Claim is proven much easier using strong induction!

**Strengthening the Inductive Hypothesis**

- Suppose we want to prove $\forall x \in \mathbb{Z}^+. P(x)$, but proof doesn’t go through
  - **Common trick:** Prove a stronger property $Q(x)$
  - If $\forall x \in \mathbb{Z}^+. Q(x) \rightarrow P(x)$ and $\forall x \in \mathbb{Z}^+. Q(x)$ is provable, this implies $\forall x \in \mathbb{Z}^+. P(x)$
  - In many situations, strengthening inductive hypothesis allows proof to go through!

**Example**

- Prove the following theorem: “For all $n \geq 1$, the sum of the first $n$ odd numbers is a perfect square.”
- We want to prove $\forall x \in \mathbb{Z}+. P(x)$ where:
  
  $$P(n) = \sum_{i=1}^{n} 2i - 1 = k^2$$

  for some integer $k$

  - Try to prove this using induction...

**Claim is proven much easier using strong induction!**
Proof Using Strong Induction

Prove that if \( n \) is an integer greater than 1, then it is either a prime or can be written as the product of primes.

▶ Base case: same as before.
▶ Inductive step: Assume each of 2, 3, \ldots, \( k \) is either prime or product of primes.
▶ Now, we want to prove the same thing about \( k+1 \)
▶ Two cases: \( k \) is either (i) prime or (ii) composite
▶ If it is prime, property holds.

Proof, cont.

▶ If composite, \( k+1 \) can be written as \( pq \) where \( 2 \leq p, q \leq k \)
▶ By the IH, \( p, q \) are either primes or product of primes.
▶ Thus, \( k+1 \) can also be written as product of primes
▶ Observe: Much easier to prove this property using strong induction!

A Word about Base Cases

▶ In all examples so far, we had only one base case
▶ i.e., only proved the base case for one integer
▶ In some inductive proofs, there may be multiple base cases
▶ i.e., prove base case for the first \( k \) numbers
▶ In the latter case, inductive step only needs to consider numbers greater than \( k \)

Example

▶ Prove that every integer \( n \geq 12 \) can be written as \( n = 4a + 5b \) for some non-negative integers \( a, b \).
▶ Proof by strong induction on \( n \) and consider 4 base cases
▶ Base case 1 (\( n=12 \)): \( 12 = 3 \cdot 4 + 0 \cdot 5 \)
▶ Base case 2 (\( n=13 \)): \( 13 = 2 \cdot 4 + 1 \cdot 5 \)
▶ Base case 3 (\( n=14 \)): \( 14 = 1 \cdot 4 + 2 \cdot 5 \)
▶ Base case 4 (\( n=15 \)): \( 15 = 0 \cdot 4 + 3 \cdot 5 \)

Example, cont.

Prove that every integer \( n \geq 12 \) can be written as \( n = 4a + 5b \) for some non-negative integers \( a, b \).

▶ Inductive hypothesis: Suppose every \( 12 \leq i \leq k \) can be written as \( i = 4a + 5b \).
▶ Inductive step: We want to show \( k+1 \) can also be written this way for \( k + 1 \geq 16 \)
▶ Observe: \( k + 1 = (k - 3) + 4 \)
▶ By the inductive hypothesis, \( k - 3 = 4a + 5b \) for some \( a, b \) because \( k - 3 \geq 12 \)
▶ But then, \( k + 1 \) can be written as \( 4(a + 1) + 5b \)

Matchstick Example

▶ The Matchstick game: There are two piles with same number of matches initially
▶ Two players take turns removing any positive number of matches from one of the two piles
▶ Player who removes the last match wins the game
▶ Prove: Second player always has a winning strategy.
Matchstick Proof

- $P(n)$: Player 2 has winning strategy if initially $n$ matches in each pile
- Base case:
- Induction: Assume $\forall j. 1 \leq j \leq k \rightarrow P(j)$; show $P(k + 1)$
- Inductive hypothesis:
- Prove Player 2 wins if each pile contains $k + 1$ matches

Matchstick Proof, cont.

- Case 1: Player 1 takes $k + 1$ matches from one of the piles.
- What is winning strategy for player 2
- Case 2: Player 1 takes $r$ matches from one pile, where $1 \leq r \leq k$
- Now, player 2 takes $r$ matches from other pile
- Now, the inductive hypothesis applies $\Rightarrow$ player 2 has winning strategy for rest of the game