Part III: Induction and Recursion

One of the most powerful techniques
in mathematics and computer science

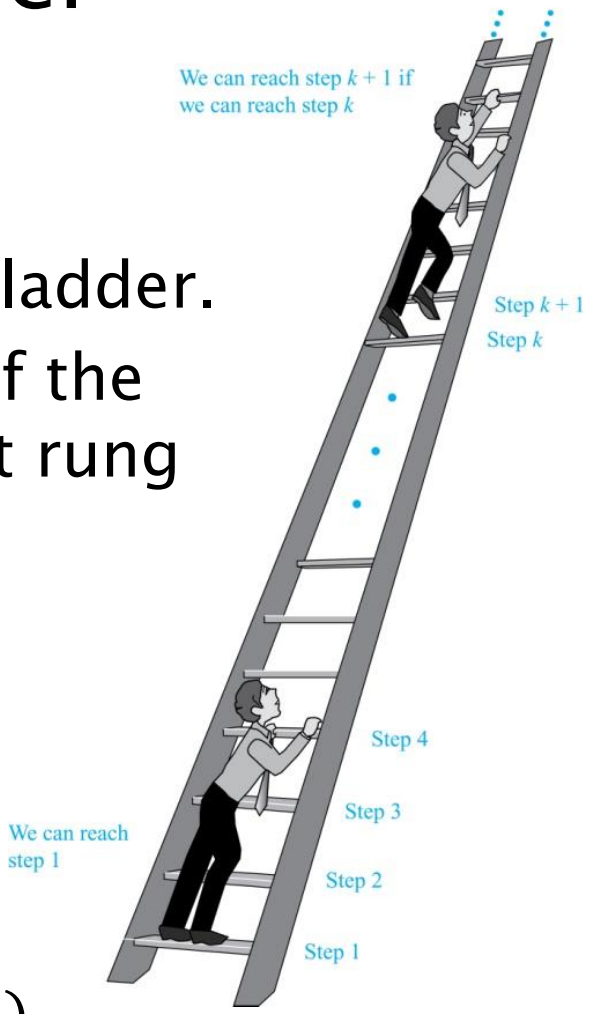
L09: Mathematical Induction

- Reading: Rosen 5.1, 5.2

Climbing an Infinite Ladder

- We are given:
  - We can reach the first rung of the ladder.
  - If we can reach a particular rung of the ladder, then we can reach the next rung
- We can conclude:
  - We can reach any rung

- In logic:
  - $P(k)$: We can reach rung k.
  - $P(1) \wedge \forall k\big(P(k) \rightarrow P(k+1)\big) \rightarrow \forall n P(n)$
  - Domain: $\mathbf{Z}^+$



Principle of Mathematical Induction

$$\forall P \left(P(1) \wedge \forall k \big(P(k) \rightarrow P(k+1) \big) \rightarrow \forall n P(n) \right)$$

- Domain of P: Any propositional function with one variable
- Domain of k, n: $\mathbf{Z}^+$
- Note that this is a second-order logic statement
- Why is it true?
  - Well, it's obvious (indeed, it is often taken as an axiom)
  - Follows from the well-ordering property:
    For any $S \subseteq \mathbf{Z}^+$, S has a least element.
  - In fact, the well-ordering property can be shown to be equivalent to the principle of induction

Validity of Mathematical Induction

Well-ordering property → mathematical induction:

- Consider any P
- We are given
  - $P(1)$
  - $\forall k\big(P(k) \rightarrow P(k+1)\big)$
- Proof by contradiction: Assume $\forall n P(n)$ is false.
- Let $S = \{i \in \mathbf{Z}^+ \mid P(i) \text{ is false}\}$
- By the well-ordering principle, S has a least element, say m.
- $m \neq 1$ since $P(1)$ is true. So $m-1 \in \mathbf{Z}^+$ and $P(m-1)$ is true.
- $P(m)$ is false and $P(m-1)$ is true. This contradicts with $\forall k\big(P(k) \rightarrow P(k+1)\big)$.

Proving Summations

- **Example**: Show that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
- **Solution**:
  - Basis: $P(1)$ is true since $1(1 + 1)/2 = 1$.
  - Inductive step: Assume true for $P(k)$, i.e., the inductive hypothesis is $\sum_{i=1}^{k} \boldsymbol{i} = \frac{k(k+1)}{2}$
  - Under this assumption,

$$\begin{aligned} 1 + 2 + \ldots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Proving Summations

- **Example**:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

- **Proof**:
  - Basis: $P(1)$ is true since $1^2 = 1$.
  - Inductive step: $P(k) \rightarrow P(k + 1)$ for every positive integer k.
  - Induction hypothesis $P(k)$:

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2$$

  - So, assuming $P(k)$, it follows that:

$$1 + 3 + \cdots + (2k + 1) = [1 + 3 + \cdots + (2k - 1)] + (2k + 1)$$
$$= k^2 + (2k + 1) \text{ (by the inductive hypothesis)}$$
$$= k^2 + 2k + 1 = (k + 1)^2$$

The Good and Bad of Induction

- The good:
  - Proofs using induction are often mechanical
- The bad:
  - Proof by induction needs a valid conjecture first
  - Offers less insight to the problem

Proving Inequalities

- **Example**: Use mathematical induction to prove that $n < 2^n$ for all positive integers n.
- **Solution**:
  - Basis: $P(1)$ is true since $1 < 2^1 = 2$.
  - Inductive step: Assume $P(k)$ holds, i.e., $k < 2^k$, for an arbitrary positive integer k.
  - Must show that $P(k+1)$ holds. Since by the inductive hypothesis, $k < 2^k$, it follows that:
    $$k + 1 < 2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$
  - Therefore $n < 2^n$ holds for all positive integers n.

Variants of Induction

- Original version

$$\forall P \left(P(1) \wedge \forall k \big(P(k) \rightarrow P(k+1) \big) \rightarrow \forall n P(n) \right)$$

  - Domain of k, n: $\mathbf{Z}^+$
- Variants:

$$\forall P \left(P(0) \wedge \forall k \big(P(k) \rightarrow P(k+1) \big) \rightarrow \forall n P(n) \right)$$

  - Domain of k, n: $\mathbf{N}$
- Variants:

$$\forall P \left(P(a) \wedge \forall k \big(P(k) \rightarrow P(k+1) \big) \rightarrow \forall n P(n) \right)$$

  - Domain of k, n: $\{a, a+1, \ldots\}$

Proving Inequalities

- **Example**: Use mathematical induction to prove that $2^n < n!$, for every integer $n \geq 4$.
- **Solution**: Let $P(n)$ be the proposition that $2^n < n!$
  - Basis: $P(4)$ is true since $2^4 = 16 < 4! = 24$.
  - Inductive step: Assume $P(k)$ holds, i.e., $2^k < k!$ for an arbitrary integer $k \geq 4$. To show that $P(k+1)$ holds:

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &< 2 \cdot k! \quad \text{(by the inductive hypothesis)} \\ &< (k+1)k! \quad \text{(since } k \geq 4\text{)} \\ &= (k+1)! \end{aligned}$$

Proving Divisibility Results

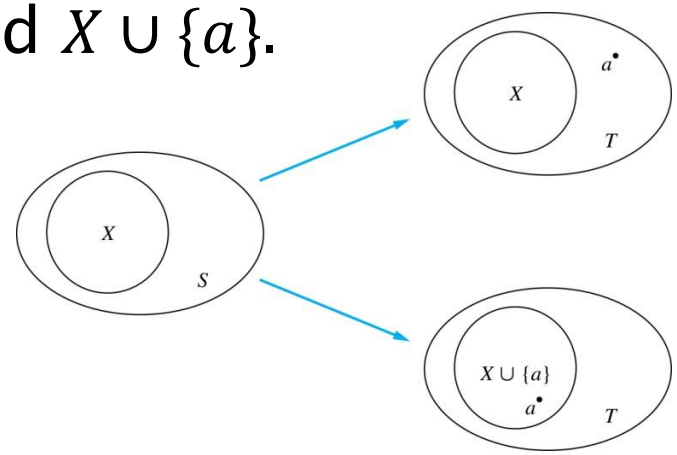
- **Example**: Use mathematical induction to prove that $n^3 - n$ is divisible by 3, for every positive integer n.
- **Solution**: Let $P(n)$ be the proposition that $3 \mid n^3 - n$
  - Basis: $P(1)$ is true since $1^3 - 1 = 0$ and $3 \mid 0$
  - Inductive step: Assume $P(k)$ holds, i.e., $3 \mid (k^3 - k)$. To show that $P(k+1)$ is true:
    $$(k+1)^3 - (k+1) = (k^3 + 3k^2 + 3k + 1) - (k+1)$$
    $$= (k^3 - k) + 3(k^2 + k)$$
  - By the inductive hypothesis, the first term $(k^3 - k)$ is divisible by 3
  - The second term is divisible by 3
  - So $P(k)$ is true.

Number of Subsets of a Finite Set

- **Example**: Use mathematical induction to show that if S is a finite set with n elements, then S has 2^n subsets.
- **Solution**: Let $P(n)$ be the proposition that a set with n elements has 2^n subsets.
  - Basis: $P(0)$ is true, because the empty set has only itself as a subset and $2^0 = 1$.
  - Inductive Step: Assume $P(k)$ is true for an arbitrary nonnegative integer k.

Proof (cnt'd)

- Let T be a set with $k+1$ elements. Pick some arbitrary element $a \in T$. Let $S = T - \{a\}$. We have $|S| = k$.
- For each subset X of S, there are exactly two subsets of T, i.e., X and $X \cup \{a\}$.



- By the inductive hypothesis, S has 2^k subsets. Since there are two subsets of T for each subset of S, the number of subsets of T is $2 \cdot 2^k = 2^{k+1}$.

Odd Pie Fight Problem

An odd number of people stand in a yard. Each person throws a pie at their nearest neighbor (assuming all mutual distances are distinct). Show that at least one person survives.

Proof

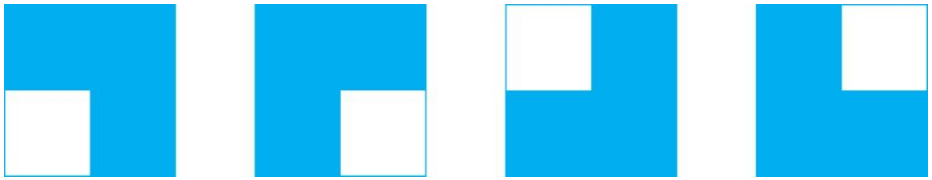
- Let $P(n)$ be the statement that there is a survivor when there are $2n + 1$ people.
- Basis: $P(1)$ is true.
  - There are $2n + 1 = 3$ people: A, B, C.
  - Without loss of generality, suppose the distance between A and B is the smallest among the 3 pairs.
  - Then, A and B throw at each other and C survives.
- Inductive step: Assume $P(k)$ is true, i.e., when there are $2k + 1$ people, there is a survivor, for an arbitrary positive integer k
  - Now we want to prove $P(k + 1)$ is true, i.e., when there are $2k + 3$ people, there is a survivor.

Proof (cnt'd)

- Idea: Need to reduce the problem from $2k + 3$ to $2k + 1$
  - Can we remove two arbitrary people?
- Let A and B be the pair of people with the smallest distance.
  - A and B must throw at each other
- Case 1: No one else throws at A or B
  - Apply the induction hypothesis on the remaining $2k + 1$ people. Done.
- Case 2: Someone else throws at A or B
  - There are $2k + 1$ people left
  - They throw $2k$ pies among themselves
  - At least one must survive

Tiling Checkerboards

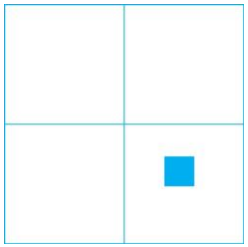
- Show that every $2^n \times 2^n$ checkerboard with one square removed can be tiled using L-shaped tiles.

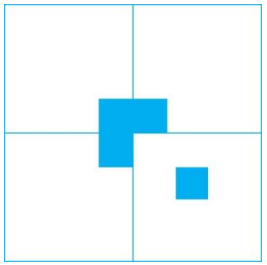


- **Solution**
  - Let $P(k)$ be the proposition that every $2^k \times 2^k$ checkerboard with one square removed can be tiled
  - Basis: $P(1)$ is true trivially
  - Inductive step: Assume $P(k)$ is true
  - Want to show that $P(k+1)$ is true.

Tiling Checkerboards

- Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed





- Look at which quadrant contains the removed square.
  - Without loss of generality, assume it is in the right-bottom quadrant
- Put a tile as shown. Then apply the induction hypothesis on each of the four quadrants.

Euclid's Division Theorem

- **Theorem:**
  For any $a \in \mathbf{Z}, d \in \mathbf{Z}^+$, there exist unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.
- **Proof** (of existence):
- Let d be any positive integer.
- Let $P(k)$ be the proposition
  $$\exists q \exists r (0 \leq r < d \wedge k = dq + r)$$
- Basis: $P(0)$ is true by taking $q = 0, r = 0$
- Inductive step: Assume $P(k)$ is true. Want to show $P(k+1)$ is true. By the induction hypothesis, there exist q, r such that $0 \leq r < d$ and $k = dq + r$. So
  $$k + 1 = dq + r + 1$$

Proof (cnt'd)

- We have
$$k + 1 = dq + r + 1$$
- If $r < d - 1$
  - Then we are done since we have found $q' = q, r' = r + 1$ such that $0 \leq r' < d$ and $k + 1 = dq' + r'$
- If $r = d - 1$
  - Let $q' = q + 1, r' = 0$. We have $k + 1 = dq' + r'$
- We have only proved the theorem for all $a \geq 0$. How about $a < 0$?
  - Can't use induction on $\mathbf{Z}$ because it doesn't satisfy the well-ordering property.
  - Idea is to prove the theorem for $\{0\} \cup \mathbf{Z}^+$ and $\{0\} \cup \mathbf{Z}^-$

Proof (cnt'd)

- Let $P(k)$ be the proposition
$$\exists q \exists r(0 \leq r < d \wedge -k = dq + r)$$
- Basis: $P(0)$ is true by taking $q = 0, r = 0$
- Inductive step: Assume $P(k)$ is true. Want to show $P(k+1)$ is true. By the induction hypothesis, there exist q, r such that $0 \leq r < d$ and $-k = dq + r$. So
$$-(k+1) = dq + r - 1$$
- If $r > 0$
  - Then we are done since we have found $q' = q, r' = r - 1$ such that $0 \leq r' < d$ and $-(k+1) = dq' + r'$
- If $r = 0$
  - Let $q' = q - 1, r' = d - 1$. We have $-(k+1) = dq' + r'$

Strong Induction

- Original version

$$\forall P\left(P(1) \wedge \forall k\big(P(k) \rightarrow P(k+1)\big) \rightarrow \forall n P(n)\right)$$

- Strong induction

$$\forall P\left(P(1) \wedge \forall k\big(P(1) \wedge \cdots \wedge P(k) \rightarrow P(k+1)\big) \rightarrow \forall n P(n)\right)$$

- It is "strong" because the induction hypothesis is stronger
  - It is easier to prove the inductive step
- In fact, these two are equivalent (both equivalent to the well-ordering property)
  - But strong induction provides more convenience for proofs.

Fundamental Theorem of Arithmetic

- **Theorem:**
  Every positive integer greater than 1 can be written as the product of primes.
- **Proof**
- Let $P(n)$ be the proposition that n can be written as a product of primes.
- Basis: $P(2)$ is true since 2 itself is prime.
- Inductive step: The inductive hypothesis is $P(j)$ is true for all integers j with $2 \leq j \leq k$. We want to show that $P(k+1)$ is true:
  - If $k+1$ is prime, then $P(k+1)$ is true.
  - Otherwise, $k+1$ is composite, i.e., $k+1 = ab$ with $2 \leq a \leq b \leq k$. By the inductive hypothesis a and b can be written as the product of primes. So $k+1$ can also be written as the product of those primes.

Two Piles of Matches Problem

- **Problem:**
  We have two piles of the same number of matches. Two players take turn to remove any positive number of matches from one of the two piles. The one who removes the last match from the two piles wins. Show that the second player can always win.

Proof

- Let $P(k)$ be the statement that the second player can win when both piles have k matches.
- Basis: $P(1)$ is true trivially.
- Inductive step: Assume $P(1), \ldots, P(k)$ are all true. Want to show that $P(k+1)$ is true.
- Suppose the first player first removes r matches from one pile, where r can be any integer $1 \leq r \leq k+1$.
- Case 1: If $r = k+1$, then second player wins by taking all matches from the other pile
- Case 2: If $r \leq k$, then the second player takes r matches from the other pile. There are $k+1-r$ matches left in both piles. By the induction hypothesis, $P(k+1-r)$ is true. So the second player can win.

Mistakes in Proofs by Induction (1)

- Let $P(n)$ be the statement that every set of n lines in the plane, no two of which are parallel, meet in a common point. Here is a "proof" that $P(n)$ is true for all positive integers $n \geq 2$.
- Proof
  - Basis: $P(2)$ is trivially true.
  - Inductive step: Assume $P(k)$ is true, i.e., every set of k lines in the plane, no two of which are parallel, meet in a common point.
    - Will show that $P(k+1)$ is true.

Proof (cnt'd)

- Consider a set of $k+1$ lines in the plane, no two parallel. We can assume these lines are distinct, otherwise $P(k+1)$ trivially holds by strong induction.
- By the inductive hypothesis, the first k of these lines must meet at a common point p_1. Similarly, the last k of these lines meet at a common point p_2.
- If p_1 and p_2 are different points, all lines containing both of them (i.e., $k-1$ lines) must be the same line since two points determine a line. This contradicts the assumption that the lines are distinct. Hence, $p_1 = p_2$ lies on all $k+1$ lines, and therefore $P(k+1)$ holds.
- **Where is the error?**
- The inductive step only holds for $k \geq 3$. Does not hold for $P(2) \rightarrow P(3)$.

Mistakes in Proofs by Induction (2)

- Below is a "proof" that $\sum_{i=1}^{n} i = O(n)$
- Proof
  - Let $P(n)$: $\sum_{i=1}^{n} i = O(n)$
  - Basis: $P(1)$ is $1 = O(1)$, trivially true.
  - Inductive step:
    - Assume $P(k)$ is true, i.e., $\sum_{i=1}^{k} i = O(k)$
    - Will show that $P(k+1)$ is true, i.e., $\sum_{i=1}^{k+1} i = O(k+1)$
    - We have $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = O(k) + k + 1 = O(k) + 1 = O(k+1)$
- Lesson learned: Don't use asymptotic notation inside induction proofs!