CS 2305: Discrete Mathematics for Computing I

Lecture 24

- KP Bhat

Conjecturing and Proving Correct a Summation Formula

Example: Conjecture and prove correct a formula for the sum of the first *n* positive odd integers. Then prove your conjecture.

Solution: We have: $1=1,\ 1+3=4,\ 1+3+5=9,\ 1+3+5+7=16,\ 1+3+5+7+9=25.$

- We can conjecture that the sum of the first *n* positive odd integers is n^2,

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

- We prove the conjecture is proved correct with mathematical induction.
- BASIS STEP: $P(1)$ is true since $1^2 = 1$.
- INDUCTIVE STEP: $P(k) \rightarrow P(k+1)$ for every positive integer k.

  Assume the inductive hypothesis holds and then show that $P(k+1)$ holds has well.

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

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

$$\begin{aligned}1+3+5+\cdots+(2k-1)+(2k+1) &= [1+3+5+\cdots+(2k-1)]+(2k+1)\\ &= k^2+(2k+1)\ (by\ the\ inductive\ hypothesis)\\ &= k^2+2k+1\\ &= (k+1)^2\end{aligned}$$

- Hence, we have shown that $P(k+1)$ follows from $P(k)$. Therefore the sum of the first *n* positive odd integers is n^2.

Proving Inequalities[1]

Example: Use mathematical induction to prove that $n < 2^n$ for all positive integers n.

Solution: Let $P(n)$ be the proposition that $n < 2^n$.

- BASIS STEP: $P(1)$ 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:

$$k+1 < 2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1} \quad \Big| \quad 1 \leq 2^k$$

Therefore $n < 2^n$ holds for all positive integers n.

Proving Inequalities₂

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 STEP: $P(4)$ 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:

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

Therefore, $2^n < n!$ holds, for every integer $n \geq 4$.

Note that here the basis step is $P(4)$, since $P(0)$, $P(1)$, $P(2)$, and $P(3)$ are all false.

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 $n^3 - n$ is divisible by 3.

- BASIS STEP: $P(1)$ is true since $1^3 - 1 = 0$, which is divisible by 3.
- INDUCTIVE STEP: Assume $P(k)$ holds, i.e., $k^3 - k$ is divisible by 3, for an arbitrary positive integer k. To show that $P(k + 1)$ follows:

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= (k^3 - k) + 3(k^2 + k)\end{aligned}$$

Let a, b, and c be integers, where $a \neq 0$. Then
(*i*) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

By the inductive hypothesis, the first term $(k^3 - k)$ is divisible by 3 and the second term is divisible by 3 since it is an integer multiplied by 3. So by part (i) of Theorem 1 in Section 4.1 , $(k + 1)^3 - (k + 1)$ is divisible by 3.

Therefore, $n^3 - n$ is divisible by 3, for every integer positive integer n.

Number of Subsets of a Finite Set[1]

Example: Use mathematical induction to show that if S is a finite set with n elements, where n is a nonnegative integer, then S has 2^n subsets.

Solution: Let $P(n)$ be the proposition that a set with n elements has 2^n subsets.

- Basis Step: $P(0)$ 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.

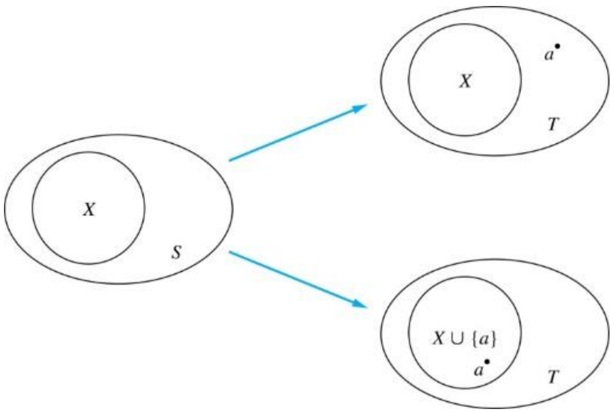
Number of Subsets of a Finite Set[2]

Inductive Hypothesis: For an arbitrary nonnegative integer k, every set with k elements has 2^k subsets.

Let T be a set with $k + 1$ elements. Let us isolate $a \in T$, an arbitrary element of T.

Clearly $T = S \cup \{a\}$, where $a \in T$ and $S = T - \{a\}$. Hence $|S| = k$.

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 $2 \cdot 2^k = 2^{k+1}$.

Guidelines: Mathematical Induction Proofs

Template for Proofs by Mathematical Induction

1. Express the statement that is to be proved in the form "for all $n \geq b$, $P(n)$" for a fixed integer b.
2. Write out the words "Basis Step." Then show that $P(b)$ is true, taking care that the correct value of b is used. This completes the first part of the proof.
3. Write out the words "Inductive Step".
4. State, and clearly identify, the inductive hypothesis, in the form "assume that $P(k)$ is true for an arbitrary fixed integer $k \geq b$."
5. State what needs to be proved under the assumption that the inductive hypothesis is true. That is, write out what $P(k + 1)$ says.
6. Prove the statement $P(k + 1)$ making use the assumption $P(k)$. Be sure that your proof is valid for all integers k with $k \geq b$, taking care that the proof works for small values of k, including $k = b$.
7. Clearly identify the conclusion of the inductive step, such as by saying "this completes the inductive step."
8. After completing the basis step and the inductive step, state the conclusion, namely, by mathematical induction, $P(n)$ is true for all integers n with $n \geq b$.

More Examples

- Self Study
  - Mathematical induction examples in the textbook on pages 339 to 345

An Incorrect "Proof" by Mathematical Induction (1)

THIS IS A FLAWED PROOF FOR MATHEMATICAL INDUCTION

Inductive Hypothesis: If X is a set consisting of n rabbits, then all rabbits in X are the same color.

BASIS STEP: For *n = 1* the claim is obviously true.

ATTEMPTED INDUCTIVE STEP: Let us assume that the result holds true for some value *k* i.e. in a set of size *k*, all rabbits will have the same color.

Let $S_1 = \{r_1, r_2, \ldots, r_k, r_{k+1}\}$ be a set consisting of k+1 rabbits.

Let us remove the last rabbit (r_{k+1}) from the set. We now get set $S_2 = \{r_1, r_2, \ldots, r_k\}$. Set S_2 has k rabbits and by our assumption all the rabbits in this set have the same color.

Let us now put the last rabbit back into the set and remove the first element (r_1) from the set. We now get set $S_3 = \{r_2, \ldots, r_k, r_{k+1}\}$. Set S_3 also has k rabbits and by our assumption all the rabbits in this set also have the same color.

The "middle" rabbits ($r_2, r_3, \ldots, r_k$) belong to both sets S_2 and S_3, so they have the same color as rabbits r_1 and r_{k+1}.

Hence all the k+1 rabbits in S_1 have the same color.

An Incorrect "Proof" by Mathematical Induction (2)

THIS IS A FLAWED PROOF FOR MATHEMATICAL INDUCTION

There must be an error in this proof since the conclusion is absurd. But where is the error?

Answer: The proof is wrong because the logic used in the inductive step breaks down when k=1.

When we remove a rabbit from the set, we get an empty set. In other words we have no "middle" rabbits (r_2, r_3, …., r_k), which are so critical in the reasoning of our proof, to play with.

Strong Induction ~~and Well-Ordering~~

Section 5.2

Strong Induction[1]

- Strong mathematical induction is similar to ordinary mathematical induction in that there is a basis step and an inductive step
- However, the inductive step shows that if P(j) is true for <u>all positive integers j not exceeding k</u>, then P(k + 1) is true.
  – For the inductive hypothesis we assume that P(j) is true for j = 1, 2,…, k.
- Taking the dominoes analogy one step further, imagine that the dominoes are arranged in increasing order of weight and a given domino requires the combined weight of all the previous dominoes toppling over before it topples over as well.

Strong Induction[2]

Strong Induction: To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, complete two steps:

- *Basis Step*: Verify that the proposition $P(1)$ is true.
- *Inductive Step*: Show the conditional statement

$$\left[P(1) \wedge P(2) \wedge \cdots \wedge P(k)\right] \rightarrow P(k+1)$$

holds for all positive integers k.

Strong Induction is sometimes called the *second principle of mathematical induction* or *complete induction*.

Strong Induction and the Infinite Ladder

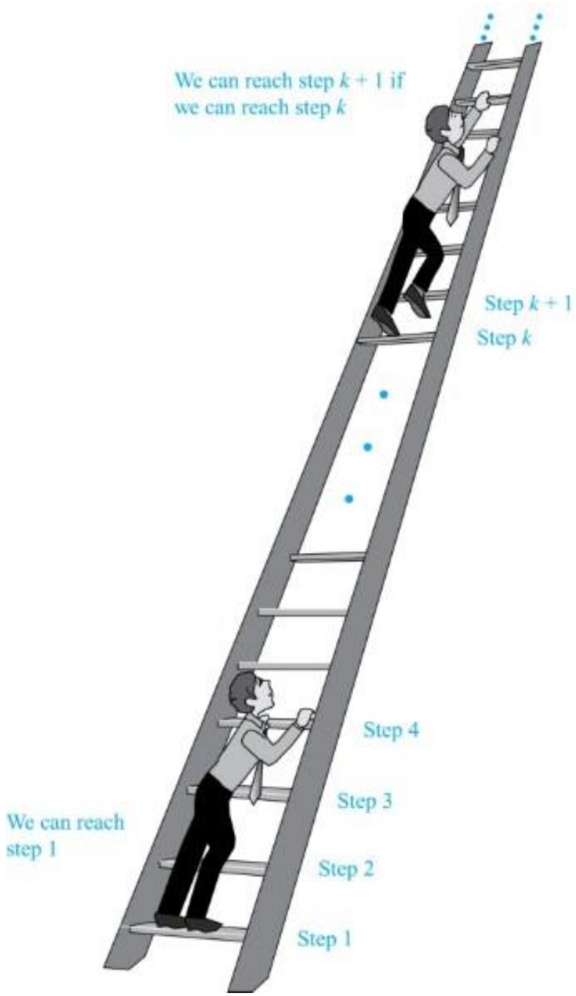
Strong induction tells us that we can reach all rungs if:

1. We can reach the first rung of the ladder.
2. For every integer k, if we can reach the first k rungs, then we can reach the $(k + 1)^{st}$ rung.

To conclude that we can reach every rung by strong induction:

- BASIS STEP: $P(1)$ holds
- INDUCTIVE STEP: Assume $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$ holds for an arbitrary integer k, and show that $P(k + 1)$ must also hold.

We will have then shown by strong induction that for every positive integer n, $P(n)$ holds, i.e., we can reach the nth rung of the ladder.



Strong Induction[3]

- Strong induction is useful in some instances where it is not apparent right away how to formulate the basis step for mathematical induction
- It can be proved that the principle of mathematical induction and strong induction are equivalent (Section 5.2, Exercise 42)
  – any result that can be proved by mathematical induction can be proved by strong induction and vice versa
  – neither proof technique is “stronger” than the other

Slightly Different Infinite Ladder Problem: Attempted Proof Using Mathematical Induction

Example: Suppose we can reach the first and second rungs of an infinite ladder, and we know that if we can reach a rung, then we can reach two rungs higher. Prove that we can reach every rung.

Solution: Prove the result using mathematical induction.

- BASIS STEP: We can reach the first step.
- ATTEMPTED INDUCTIVE STEP: The inductive hypothesis is that we can reach the k^{th} rung.

However, assuming that we have reached the k^{th} rung, we know how to reach the $(k+2)^{\mathrm{nd}}$ rung, but we don't know how to reach the $(k + 1)^{\mathrm{st}}$ rung.

Hence we <u>cannot conclude</u> that if we have reached the k^{th} rung we can reach the reach the $(k + 1)^{st}$ rung as well.

Slightly Different Infinite Ladder Problem: Proof Using Strong Induction

Example: Suppose we can reach the first and second rungs of an infinite ladder, and we know that if we can reach a rung, then we can reach two rungs higher. Prove that we can reach every rung.

Solution: Prove the result using strong induction.

- BASIS STEP: We can reach the first step.
- INDUCTIVE STEP: The inductive hypothesis is that we can reach the first k rungs, for any $k \geq 2$.

  Once we have reached the $(k-1)^{st}$ rung, we can reach two rungs higher i.e. we can reach the $(k+1)^{st}$ rung.

- Hence, we can reach all rungs of the ladder.

Which Form of Induction Should Be Used?

- We can always use strong induction instead of mathematical induction. But there is no reason to use it if it is simpler to use mathematical induction
  - you should use mathematical induction when it is straightforward to prove that $P(k) \to P(k + 1)$ is true for all positive integers k.
- Use strong induction, and not mathematical induction, when you see how to prove that $P(k + 1)$ is true from the assumption that $P(j)$ is true for all positive integers j not exceeding k, but you cannot see how to prove that $P(k + 1)$ follows from just $P(k)$
- However, as already mentioned, in theory any result that can be proved by mathematical induction can be proved by strong induction and vice versa

Proof that mathematical induction and strong induction are equivalent

The strong induction principle clearly implies ordinary induction, for if one has shown that $P(k) \to P(k+1)$, then it automatically follows that $[P(1) \wedge \cdots \wedge P(k)] \to P(k+1)$; in other words, strong induction can always be invoked whenever ordinary induction is used.

Conversely, suppose that $P(n)$ is a statement that one can prove using strong induction. Let $Q(n)$ be $P(1) \wedge \cdots \wedge P(n)$. Clearly $\forall n P(n)$ is logically equivalent to $\forall n Q(n)$. We show how $\forall n Q(n)$ can be proved using ordinary induction. First, $Q(1)$ is true because $Q(1) = P(1)$ and $P(1)$ is true by the basis step for the proof of $\forall n P(n)$ by strong induction. Now suppose that $Q(k)$ is true, i.e., $P(1) \wedge \cdots \wedge P(k)$ is true. By the proof of $\forall n P(n)$ by strong induction it follow that $P(k+1)$ is true. But $Q(k) \wedge P(k+1)$ is just $Q(k+1)$. Thus we have proved $\forall n Q(n)$ by ordinary induction.

Not on the exam

Completion of the proof of the Fundamental Theorem of Arithmetic

Example: Show that if n is an integer greater than 1, then n can be written as the product of primes.

Solution: Let $P(n)$ be the proposition that n can be written as a product of primes.

- BASIS STEP: $P(2)$ is true since 2 itself is prime.
- INDUCTIVE STEP: The inductive hypothesis is $P(j)$ is true for all integers j with $2 \leq j \leq k$. To show that $P(k + 1)$ must be true under this assumption, two cases need to be considered:
  - If $k + 1$ is prime, then $P(k + 1)$ is true.
  - Otherwise, $k + 1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k + 1$. By the inductive hypothesis a and b can be written as the product of primes and therefore $k + 1$ can also be written as the product of those primes.

Hence, it has been shown that every integer greater than 1 can be written as the product of primes.