CS201: Data Structures and Discrete Mathematics I

Mathematical Induction

Outline

- Proof techniques
- Inductive proofs and examples

Proof Techniques

- There are a number of techniques to prove or to disprove an conjecture.
  - Disproof by counterexample
  - Exhaustive proof
  - Direct proof
  - Proof by contraposition
  - Proof by contradiction
  - Proof by induction

A conjecture

- In practice or research, you observe a number of cases in which something Q is true whenever some condition P is true.
- On the basis of these experiences, you can formulate a conjecture:
  - If P is true then Q is true.
- However, you need to prove it by applying some deductive reasoning. That is, to verify the truth or falsity of your conjecture. You produce a proof.
- When it is proved, the conjecture becomes a theorem. Or, you can find a counterexample to disapprove the conjecture, a case in which P is true but Q is false.

Disproof by counterexample

- To disprove a conjecture by giving a counterexample.
  - Prove or disprove the conjecture "For every positive integer n, $n! \leq n^2$"

$n = 1$, $n! = 1$, $n^2 = 1$ yes

$n = 2$, $n! = 2$, $n^2 = 4$ yes

$n = 3$, $n! = 6$, $n^2 = 9$ yes

$n = 4$, $n! = 24$, $n^2 = 16$ no (a counterexample)

Exhaustive Proof

- While “disproof by counterexample” always works, “proof by example” seldom does.
- However, when the conjecture is an assertion about a finite collection. We can prove the conjecture by showing that for each member of the collection it is true.
  - “if an integer between 1 to 13 is divisible by 6, then it is also divisible by 3”

Proof: 6 is divisible by 6, it is also divisible by 3

12 is divisible by 6, it is also divisible by 3

1,2,3,4,5,7,8,9,10,11,and 13: not divisible by 6.

Direct proof

- To prove $P \rightarrow Q$, (if P is true, then Q is true), the obvious approach is the direct proof, assume the hypothesis P and deduce the conclusion Q.
  - "if x and y are even integers, then the product xy is also an even integer"

Proof: $x = 2m$, $y=2n$, $xy=2m2n=2(2mn)$.

Proof by contraposition

- Sometimes, it is hard to directly prove the conjecture $P \rightarrow Q$, it may be easier to prove $\neg Q \rightarrow \neg P$ (proof by contraposition). $\neg Q \rightarrow \neg P$ is the *contrapositive* of $P \rightarrow Q$.
  - "for an integer n, if n^2 is odd, then n is odd"
  - We can prove it by showing "if n is even, then n^2 is even"
  - (Which we have done previously.)

Proof by contradiction

- Assuming that the conjecture is false and showing that the assumption implies that some known property is false.
  - "If $x + x = x$, then $x = 0$"

  Proof: Assume $x + x = x$ and $x \neq 0$,

  then $2x = x$ and since $x \neq 0$, we can divide both sides of $2x = x$ by x. We obtain $2 = 1$,

  which is false.

Is this proof correct? Why?

Suppose a, b, c are real numbers and $a > b$ if $ac <= bc$ then $c <= 0$.

Proof: Suppose $c > 0$. Then we can multiply both sides of the given inequality $a > b$ by c and conclude that $ac > bc$. Therefore if $ac <= bc$ then $c <= 0$.

Proof by induction

Principle of Mathematical Induction

Let $P(n)$ be a property that is defined for integer n, and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.
2. For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then, the statement:

for all integers $n \geq a$, $P(n)$ is true.

- Proof by induction is particularly useful in computer science.

How to prove by induction?

- It has two standard steps:
  1. Base case: prove that the theorem is true for some small value(s).
  2. Inductive case: (1) assuming an inductive hypothesis, i.e., assuming the theorem is true for all cases up to some limit k, and (2) using the assumption to prove that the theorem is true for the next value, typically k+1.

Inductive proof: Example 1

Prove: $$\sum_{i=0}^{n} i = n(n+1)/2$$

Proof:

- Base case: n = 0, it is true as 0 = 0(0+1)/2
- Inductive case:
  – assume that the theorem is true up to i=k, i.e.,
  $$\sum_{i=0}^{k} i = k(k+1)/2$$
  – prove that the theorem is true for k+1, i.e.,
  $$\sum_{i=0}^{k+1} i = (k+1)(k+2)/2$$

Inductive proof: Example 1

$$\sum_{i=0}^{k+1} i = k+1+\sum_{i=0}^{k} i$$

$$= k(k+1)/2 + (k+1)$$

Using induction hypothesis

$$= (k+1)(k+2)/2$$

$$= RHS$$

Inductive proof: Example 2

Prove: $1+2+2^2+\ldots+2^n = 2^{n+1}-1$

Proof:

- Base case: $1 + 2 = 2^{1+1}-1$ (also $1 = 2^{0+1}-1$)
- Inductive case: assume

  $1+2+2^2+\ldots+2^k = 2^{k+1}-1$

  We want to show $1+2+2^2+\ldots+2^{k+1} = 2^{k+2}-1$.

  $1+2+2^2+\ldots+2^{k+1} = 1+2+2^2+\ldots 2^k+2^{k+1}$

  $= 2^{k+1}-1 + 2^{k+1}=2^{k+2}-1$

Inductive proof: Example 3

Theorem: Any denomination $n \geq 4$ (n is an integer) can be formed using \$2 and \$5 coins.

Proof:

- Base case: $n = 4$, use two \$2 coins.
- Inductive case: let $n = k + 1$ for $k \geq 4$
  - Hypothesis: assume collection C of \$2 and \$5 coins makes up k
  - If C contains two \$2 coins, replace them with a \$5
  - If not, C contains at least one \$5 coin,

    Replace one \$5 coin with three \$2 coins.

Two principles of induction

- First principle
  - Base case: the theorem is true
  - Assume that for all k, the theorem is true, and we can show that the theorem is also true for k+1.
- Second principle
  - Base case: the theorem is true
  - Assume that for all k, the theorem is true for any case from the base case to k, and we can show that the theorem is also true for k+1.

The first and the second principles are equivalent

Example 4: first principle proof

Prove: any amount of postage greater than or equal to 8 cents can be built using only 3-cent and 5 cent stamps.

Proof:

- Base case: $n = 8$, $3+5 = 8$.
- Inductive case: let $n = k + 1$ for $k \geq 8$
  - Hypothesis: assume collection C of 3 and 5 cents makes up k
  - If C contains one 5-cent, replace it with two 3-cents.
  - If not, C must contain at least three 3-cents,
    Replace three 3-cents with two 5-cents.

Example 4: second principle proof

- Base case: for $n = 8$, $3+5 = 8$. We also show two more cases, $n = 9$ $(= 3+3+3)$, and $n = 10$ $(= 5+5)$.
- Inductive case:
  - Hypothesis: assume theorem is true for any r, $8 \le r \le k$, and consider the theorem for $k+1$.
  - We can assume $k + 1 \ge 11$.

  By induction hypothesis, the theorem is true for $k-2$.

  Then, by adding a 3 to $k-2$, we obtain $k+1$. This shows that $k+1$ is a sum of 3s and 5s. Since $k-2 \ge 8$, we are done!

Question: why do we need the cases 9 and 10?

More examples

Prove that for any positive integer n, the number 2^{2n} -1 is divisible by 3.

Proof:

- Base case: $2^{2(1)} - 1 = 4 - 1 = 3$ is divisible by 3.
- Inductive case: assume $2^{2k} - 1$ is divisible by 3, which means $2^{2k} - 1 = 3m$ for some integer m, or $2^{2k} = 3m + 1$. We want to show that

$2^{2(k+1)} - 1$ is divisible by 3.

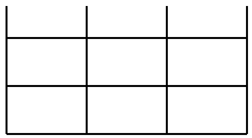
$$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2\, 2^{2k} - 1$$

$$= 2^2\,(3m+1) - 1 = 12m + 4 - 1 = 3(4m+1).$$

More examples

Prove that a straight fence with n fence posts has n-1 sections for any $n \geq 1$.

Proof:



- Base case: 1 post has 0 section
- Inductive case: assume at k fence posts form k-1 sections. We need to prove a fence with k+1 fence posts has k sections.

  We can chop off the last post and the last section. Then we have k fence post case with k-1 sections. Therefore, the original fence had k sections.

More examples

Prove: Every positive integer greater than 1 can be factored into primes; eg.,

$18 = 2 \cdot 3 \cdot 3$ and $1001 = 7 \cdot 11 \cdot 13$

Proof:

- Base case: $n = 2$ is a prime
- Inductive case: assume for n from 2 up to k, the theorem is true. We show that for $n = k+1$ the theorem is true.

  if $k+1$ is a prime, it is proven

  if $k+1$ is not a prime, by definition, $n=k+1 = r \cdot s$

  ….

What is flaw?

Theorem: All people have the same hair color.

Let T stands for the theorem. We prove T by induction as follows.

(c) Base case: T holds for n = 1. This is trivially true because a group of size 1 contains just one person, and he/she has the same hair color as himself/herself.

(b) Inductive case:

(1) Induction hypothesis: suppose T holds for n = k. That is, in any group with k persons, everyone has the same hair color.

(2) Inductive step: prove that T holds for n = k + 1. Consider a group G with k + 1 persons.

i. Remove a person p from G, let G' be the rest of the group. G' contains k persons, and by inductive hypothesis (step (1)), everyone in G' has the same hair color.

ii. Remove a different person p' from G, and let G'' be the rest of the group. G'' contains k persons, and by inductive hypothesis (step (1)), everyone in G'' has the same hair color.

From the two steps, we conclude that everyone in G has the same hair color

Again, what is wrong?

Consider 0-1 sequences in which 1's may not appear consecutively, except in the rightmost two positions. E.g., 0010100, and 1000011 are correct, and 0011000 is not. Prove that there are 2^n allowed sequence of length n.

Proof: Let N_i be the number of allowed sequences of size i.

base case: sequence of length 1. Then we have 2. Correct!!

Inductive case: assume the theorem is true for k.

Take any allowed sequence of length k, we may append either 0 or 1 at the right end – in the latter case, we may create 11 in the last two position, but that is okay. Therefore,

the number of sequence of k+1 is:

$N_{k+1} = 2N_k = 2\ 2^n = 2^{n+1}$.

Why is proof by induction correct?

- Let us prove it.

The Well-ordering principle: Any non-empty subset of Z_+ (any set of elements from Z_+) contains a smallest element.

Theorem: (Principle of mathematical induction) Let S(n) denote a mathematical statement (or set of statements) that involves one or more occurrences of the symbol n, which represent a positive integer.

(a) If S(1) is true; and

(b) If whenever S(k) is true for some k in Z_+, the truth of S(k+1) is implied by the truth of S(k);

Then S(n) is true for all n in Z_+

Prove by contradiction

- Let S(n) be such a statement satisfying conditions (a) and (b).
- Assume that for some values of n, S(n) is false.
- By the Well-Ordering Principle, there must be a smallest n for which S(n) is false. Let us denote this smallest n by r.
  - Since S(1) is true (condition (a)), $r \neq 1$. Then, $r - 1$ must be in Z_+ (i.e., r-1 is a positive integer).
  - Since r is the smallest value of n for which S(n) is false, then S(r-1) must be true. By condition (b), we obtain that $S((r-1) + 1) = S(r)$ is true, which contradicts that S(r) is false. Consequently, there is no value of n for which S(n) is false.

Which is more probable?

- Judy is thirty-three, unmarried, and quite assertive. A magna cum laude graduate, she majored in political science in college and was deeply involved in campus social affairs, especially in anti-discriminations and anti-nuclear issues. Which statement is more probable:
  1. Judy works as a bank teller.
  2. Judy works as a bank teller and is active in the feminist movement.

A joke

- A man who travels a lot was concerned about the possibility of a bomb on board his plane. He determined the probability of this, found it to be low but not low enough for him, so now he always travels with a bomb in his suitcase. He reasons that the probability of two bombs being on board would be infinitesimal.