Proofs

Debarka Sengupta

Motivation

"Mathematical proofs, like diamonds, are hard and clear, and will be touched with nothing but strict reasoning." -John Locke

Fundamental approaches

- Mathematical proofs are necessary in CS
- You must always (try to) prove that your algorithm
  - terminates
  - is sound, complete, optimal
  - finds optimal solution
- You may also want to show that it is more efficient than another method
- Proving certain properties of data structures may lead to new, more efficient or simpler algorithms
- Arguments may entail assumptions. You may strive to prove that the assumptions are valid

Fundamental approaches

1. Direct proof or proof by construction
2. Proof by induction
3. Proof by contradiction

Direct proof

Def. A direct proof is a sequence of statements which are either givens or deductions from previous statements, and whose last statement is the conclusion to be proved.

Outline.

1. Assume P is true
2. Demonstrate that Q must follow from P.

Example 1 - Direct Proof

Theorem. If n is even, so is n^2.

Proof sketch.

1. Assume n is an even number
2. $n = 2k$
3. $n^2 = 4k^2 = 2(2k^2) = 2j$

Example 1 - Direct Proof

Proof sketch.

1. Assume n is an even number
2. $n = 2k$
3. $n^2 = 4k^2 = 2(2k^2) = 2j$

Example 2 - Direct Proof

Theorem. Let a,b,c,d be integers. If $a > c$ and $b > c$, then $\mathrm{MAX}(a, b) - c$

is always positive.

Example 2 - Direct Proof

Proof sketch.

1. We are not sure about the relationship between a and b
2. Case 1: $a > b \Rightarrow MAX(a,b) = a \Rightarrow MAX(a,b)-c = a - c$. Since $a>c$, we can safely say $a - c > 0$
2. Case 2: continue ...

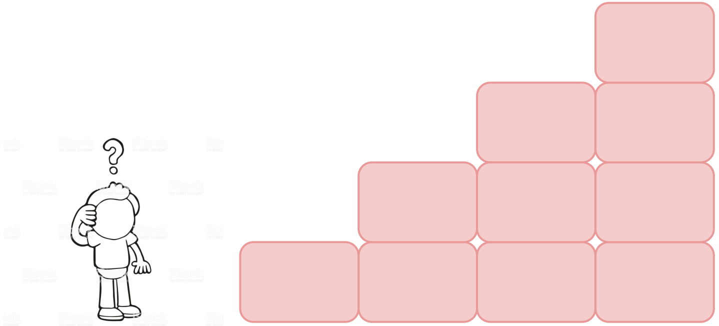
Practice problem 1 - Direct Proof

Theorem. Sum of first n integers is n(n+1)/2

Practice problem 1 - Direct Proof

Proof sketch. If we take the first and last terms of the series, since they are 1 and n, of course they sum to n+1. If we take the second term and next-to-last term, since they are 2 and n−1, they also sum to n+1. Likewise for the third term and third-from-the-end term. We can go on and pair up terms like this, such that there are n/2 pairs that each sum to n+1, for a total sum of (n+1)n/2. You can check for yourself that this is true even if n is odd (and so the middle value of the series has no partner).

Induction



To climb

1. You need to be able to climb the first step (It is not same as 2 since you are starting from plane, not step)

2. From any step, you should be able to climb the next step

Proof by induction

Outline.

1. (Basis) Show that $P \Rightarrow Q$ is valid for a specific element k in S.
2. (Inductive Hypothesis) Assume that $P \Rightarrow Q$ for some element n in S.
3. Demonstrate that $P \Rightarrow Q$ for the element $n + 1$ in S.
4. Conclude that $P \Rightarrow Q$ for all elements greater than or equal to k in S.

Example 1 - Proof by Induction

Theorem. 2 ¢ and 5 ¢ stamps can be used to form any value (for values ≥ 4).

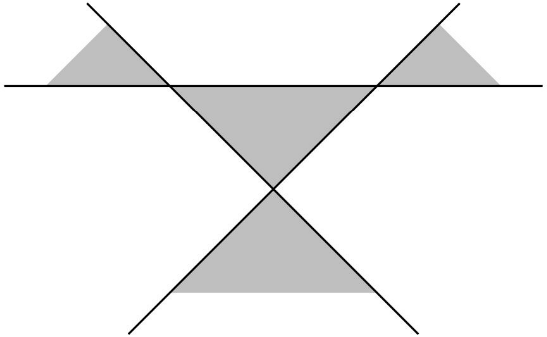
Example 1 - Proof by induction

Proof sketch.

1. Base case is trivial (take 2 pieces of 2 ¢)
2. Assuming n-1 can be made such that n-1 ≥ 4
   a. Case 1: 5 ¢ not present. In that case add 5 ¢ , remove 2 pieces of 2 ¢
   b. Case 2: Replace a 5 ¢ by 3 pieces of 2 ¢

Practice problem 1 - Proof by Induction

Theorem. The set of regions formed by n infinite lines in the plane can be two-colored (each line segment have contrasting colors on both sides).



Practice problem 1 - Proof by Induction

Proof sketch.

1. Base case is trivial (draw a line)
2. Assume n-1 lines produce regions 2-colorable
3. If a new line is added
   a. Observation 1. The new line might run through some unicolor regions leaving two sides of it (as part of at least some regions) colored by same color
   b. Two sides independently are perfectly 2-colored

Practice problem 1 - Proof by Induction

Proof sketch continued ...

All we need to do is to flip the colors of the regions on one of the sides of the line segment. Due to this construction, both sides still remain perfectly 2-colored. Moreover, now there's no chance to have same color on either side of the line at any place.

Proof by contradiction

Philosophy. A proposition can be either true or false, not both

Proof by contradiction

The simplest way to **disprove** a theorem or statement is to find a counterexample to the theorem. Unfortunately, **no number of examples supporting a theorem is sufficient** to prove that the theorem is correct. However, there is an approach that is **vaguely similar** to **disproving by counterexample**, called Proof by Contradiction. To prove a theorem by contradiction, we first assume that the theorem is false. We then find a logical contradiction stemming from this assumption. If the logic used to find the contradiction is correct, then the only way to resolve the contradiction is to recognize that the assumption that the theorem is false must be incorrect. That is, we conclude that the theorem must be true.

Example 1 - Proof by contradiction

Theorem. There is no largest integer.

Example 1 - Proof by contradiction

Proof sketch.

1. Assume there's a largest integer B ("Biggest")
2. C = B + 1 is also an integer since two integers are added to form C
3. C > B