Strategies for Proofs

'La Clairvoyance' - René Magritte

Discrete Structures (CS 173) Lecture 3

Gul Agha

Slides based on Derek Hoiem, University of Illinois

Logistics

- Moodle Activity tonight.. Due Wednesday
- HW 1 to be released today
- Remember your discussion section Friday

Goals of this lecture

- Introduce Proof
- Become familiar with various strategies for proofs

Are these conclusions valid, why?

Assume: If it rains and I forget my umbrella, then I will get wet.

1. I am wet; therefore it rained, and I forgot my umbrella.
2. It rained, and I am wet; therefore, I forgot my umbrella.
3. I am not wet; therefore, it rained, but I didn't forget my umbrella.
4. I forgot my umbrella; therefore, I will get wet.
5. I'm not wet; therefore, it didn't rain, or I brought my umbrella.

Proving universal statements

Claim: *For any integers a and b, if a and b are odd, then ab is also odd*.

Definition: integer a is *odd* iff $\mathrm{a} = 2\mathrm{m} + 1$ for some integer m

overhead

Approach to proving universal statements

1. State the supposition (hypothesis) and define any variables
2. Expand definitions such as “odd” or “rational” into their technical meaning (if necessary)
   - For clarity, state the definition being used
3. Manipulate expression until conclusion is verified by a simple statement
   - E.g., $(x + 1)^2 \geq 0$ because any squared real is non-negative.
4. End with “This is what was to be shown.” or “*QED*” to make it obvious that the proof is finished

- Tip: work out the proof on scratch paper first, then rewrite it in a clear, logical order with justification for each step.

Proving universal statements

Claim: *For any real k, if k is rational, then k^2 is rational*.

Definition: real k is *rational* iff $\mathrm{k} = \frac{\mathrm{m}}{\mathrm{n}}$ for some integers m and n, with $\mathrm{n} \neq 0$.

overhead

Things to be careful of

Don't …

- assume the conclusion is true and prove that the conclusion is true
- assume the conclusion is true and prove that the hypothesis is true
- use the same name for different variables within your proof

Do …

- work your way from the hypothesis to the conclusion without making any additional assumptions
- clearly define your variables (e.g., "where m is an integer")
- Sometimes it is easier to look at the conclusion and figure out what you need to prove it, and to then derive what is needed from the hypothesis

Proving universal statements

Claim: *For all integers n,* $4(n^2 + n + 1) - 3n^2$ *is a perfect square.*

Definition: k is a *perfect square* iff $k = m^2$ for some integer m

overhead

Proving universal statements

Claim: *The product of any two rational numbers is a rational number.*

Definition: real k is *rational* iff $k = \frac{m}{n}$ for some integers m and n, with $n \neq 0$.

overhead

Take home messages

- Propositions with “for all” and “there exists” can be encoded with *quantifiers*
- Remember rules for negation and equivalence of quantifiers
- Universal proofs are solved by
  1. Stating supposition
  2. Expanding definitions
  3. Manipulating expressions to reach conclusion
  4. Stating that the claim has been shown

Review: proving universal statements

Claim: *For any integer a, if a is odd, then a^2 is also odd*.

Definition: integer a is *odd* iff $a = 2m + 1$ for some integer m

overhead

Proving existential statements

Claim: *There exists a real number x, such that* $|x^3| < x^2$

overhead

Disproving existential statements

Claim to disprove: There exists a real $x, x^2 - 2x + 1 < 0$

$$\sim\left(\exists x\ P(x)\right) \equiv \forall x \sim P(x)$$

overhead

Disproving universal statements

Claim to disprove: For all real x, $(x+1)^2 > 0$

$$\sim\left(\forall x\ P(x)\right) \equiv \exists x\ \sim P(x)$$

overhead

Proof by cases

Claim: For every real x, if $|x + 7| > 8$, then $|x| > 1$

A deceptively difficult proof

Fermat's conjecture: 26 is the only number sandwiched between a perfect square and a perfect cube.

Rephrasing claims

Claim: There is no integer k, such that k is odd and k^2 is even.

Proof by contrapositive

Claim: For all integers a and b,

$$(a + b \geq 15) \rightarrow (a \geq 8 \vee b \geq 8)$$

Proof strategies

1. Does this proof require showing that the claim holds for all cases or just an example?
   - Show all cases: prove universal, disprove existential
   - Example: disprove universal, prove existential

2. Can you figure a straightforward solution?
   - If so, sketch it and then write it out clearly, and you're done

3. If not, try to find an equivalent form that is easier
   a) Divide into subcases that combine to account for all cases
      - OR in hypothesis is a hint that this may be a good idea

   b) Try the contrapositive
      - OR in conclusion is a hint that this may be a good idea

   c) More generally rephrase the claim: convert to propositional logic and manipulate into something easier to solve

More proof examples

Claim: For integers j and k, if j is even or k is even, then jk is even.

Definition: integer a is even iff $a = 2m$ for some integer m

What is the best proof strategy for each claim?

1. For integers j and k, if j is even or k is even, then jk is even.
2. If $x + y$ is even, then x and y are either both even or both odd.
3. Disprove that if $x = a/b$ is rational, then a and b are also rational.
4. For all integers k, if $3k + 5$ is even, then k is odd.

A. *Direct proof with cases*

B. *Proof by contrapositive*

C. *Proof by example or counter-example*

D. *Direct proof without cases*

More proof examples

Claim: For all integers k, if $3k + 5$ is even, then k is odd.

More proof examples

Disprove: For all real k, if k is rational, then $\frac{k^3}{k}$ is rational.

More complex proof

Claim: For all integers x, if x is odd, then $x = 4k + 1$ or $x = 4k - 1$ for some integer k.

(Note, this requires knowing a little about modular arithmetic.)

Next week: number theory