Department of Computer & Information Sciences
Pakistan Institute of Engineering and Applied Sciences

Mathematical Preliminaries

Based on slides by Costas Busch [http://csc.lsu.edu/~busch]
Umar Faiz
http://www.pieas.edu.pk/umarfaiz/cis317

Mathematical Proof

- A reasoned argument
- Based on knowns

Proof methods

We will discuss ten proof methods:

1. Direct proofs
2. Indirect proofs
3. Vacuous proofs
4. Trivial proofs
5. Proof by contradiction
6. Proof by cases
7. Proofs of equivalence
8. Existence proofs
9. Uniqueness proofs
10. Counterexamples

1. Direct proofs

Consider an implication: $p \rightarrow q$

If p is false, then the implication is always true

Thus, show that if p is true, then q is true

To perform a direct proof, assume that p is true, and show that q must therefore be true

Direct proof

Example:

Show that the square of an even number is an even number

Rephrased: if n is even, then n^2 is even

Assume n is even

Thus, $n = 2k$, for some k (definition of even numbers)

$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$

As n^2 is 2 times an integer, n^2 is thus even

2. Indirect proofs

Consider an implication: $p \rightarrow q$

It's contrapositive is $\neg q \rightarrow \neg p$

Is logically equivalent to the original implication!

If the antecedent ($\neg q$) is false, then the contrapositive is always true

Thus, show that if $\neg q$ is true, then $\neg p$ is true

To perform an indirect proof, do a direct proof on the contrapositive

Indirect proof example

If n^2 is an odd integer then n is an odd integer

Prove the contrapositive:

If n is an even integer, then n^2 is an even integer

Proof:

n=2k for some integer k (definition of even numbers)

$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$

Since n^2 is 2 times an integer, it is even

Which to use

When do you use a direct proof versus an indirect proof?

If it's not clear from the problem, try direct first, then indirect second

If indirect fails, try the other proofs

Example of which to use

Rosen, section 1.5, question 21

Prove that if n is an integer and n^3+5 is odd, then n is even

Via direct proof

$n^3+5 = 2k+1$ for some integer k (definition of odd numbers)

$n^3 = 2k-4$

???!!!..............

Direct proof didn't work out. Next up: indirect proof

$$n = \sqrt[3]{2k-4}$$

Example of which to use

Rosen, section 1.5, question 21 (a)

Prove that if n is an integer and n^3+5 is odd, then n is even

Via indirect proof

Contrapositive: If n is odd, then n^3+5 is even

Assume n is odd, and show that n^3+5 is even

n=2k+1 for some integer k (definition of odd numbers)

$n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$

As $2(4k^3+6k^2+3k+3)$ is 2 times an integer, it is even

10

3. Vacuous proofs

Consider an implication: $p \rightarrow q$

If it can be shown that p is false, then the implication is always true

By definition of an implication

Note that you are showing that the antecedent is false

Vacuous proof example

Consider the statement:

- All Software Engineering majors in BS (CIS) are female
- Rephrased: If you are a Software Engineering and you are in BS (CIS), then you are female

Since there are no criminology majors in this class, the antecedent is false, and the implication is true

4. Trivial proofs

Consider an implication: $p \rightarrow q$

If it can be shown that q is true, then the implication is always true

- By definition of an implication

Note that you are showing that the conclusion is true

Trivial proof example

Consider the statement:

- If you are tall and are registered in 'Theory of Automata' course, then you are a student

Since all people in 'Theory of Automata' course are students, the implication is true regardless

5. Proof by contradiction

Given a statement p, assume it is false

- Assume $\neg p$

Prove that $\neg p$ cannot occur

- A contradiction exists

Given a statement of the form $p \rightarrow q$

- To assume it's false, you only have to consider the case where p is true and q is false

Proof by contradiction example

Rosen, section 1.5, question 21 (b)

- Prove that if n is an integer and n^3+5 is odd, then n is even
- Rephrased: If n^3+5 is odd, then n is even
  - Thus, p is "n^3+5" is odd, q is "n is even"

Assume p and $\neg q$

- Assume that n^3+5 is odd, and n is odd

Since n is odd:

- $n=2k+1$ for some integer k (definition of odd numbers)
- $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$
- As $n = 2(4k^3+6k^2+3k+3)$ is 2 times an integer, n must be even
- Thus, we have concluded q

Contradiction!

- We assumed q was false, and showed that this assumption implies that q must be true
- As q cannot be both true and false, we have reached our contradiction

16

6. Proof by cases

Show a statement is true by showing all possible cases are true

Thus, you are showing a statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

is true by showing that:

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

7. Proofs of equivalences

This is showing the definition of a bi-conditional

Given a statement of the form "p if and only if q"

- Show it is true by showing $(p \rightarrow q) \wedge (q \rightarrow p)$ is true

Proofs of equivalence example

Rosen, section 1.5, question 40

- Show that $m^2=n^2$ if and only if m=n or m=-n
- Rephrased: $(m^2=n^2) \leftrightarrow [(m=n)\vee(m=-n)]$

Need to prove two parts:

- $[(m=n)\vee(m=-n)] \rightarrow (m^2=n^2)$
  - Proof by cases!
  - Case 1: $(m=n) \rightarrow (m^2=n^2)$
    - $(m)^2 = m^2$, and $(n)^2 = n^2$, so this case is proven
  - Case 2: $(m=-n) \rightarrow (m^2=n^2)$
    - $(m)^2 = m^2$, and $(-n)^2 = n^2$, so this case is proven
- $(m^2=n^2) \rightarrow [(m=n)\vee(m=-n)]$
  - Subtract n^2 from both sides to get $m^2-n^2=0$
  - Factor to get $(m+n)(m-n) = 0$
  - Since that equals zero, one of the factors must be zero
  - Thus, either m+n=0 (which means m=n) or m-n=0 (which means m=-n)

8. Existence proofs

Given a statement: $\exists x\ P(x)$

We only have to show that a P(c) exists for some value of c

Two types:

- Constructive: Find a specific value of c for which P(c) exists
- Nonconstructive: Show that such a c exists, but don't actually find it
  - Assume it does not exist, and show a contradiction

Constructive existence proof example

Show that a square exists that is the sum of two other squares

- Proof: $3^2 + 4^2 = 5^2$

Show that a cube exists that is the sum of three other cubes

- Proof: $3^3 + 4^3 + 5^3 = 6^3$

Non-constructive existence proof

Rosen, section 1.5, question 50

Prove that either $2*10^{500}+15$ or $2*10^{500}+16$ is not a perfect square

- A perfect square is a square of an integer
- Rephrased: Show that a non-perfect square exists in the set $\{2*10^{500}+15, 2*10^{500}+16\}$

Proof: The only two perfect squares that differ by 1 are 0 and 1

- Thus, any other numbers that differ by 1 cannot both be perfect squares
- Thus, a non-perfect square must exist in any set that contains two numbers that differ by 1

9. Uniqueness proofs

- A theorem may state that only one such value exists
- To prove this, you need to show:
  - Existence: that such a value does indeed exist
    - Either via a constructive or non-constructive existence proof
  - Uniqueness: that there is only one such value

10. Counterexamples

Given a universally quantified statement, find a single example which it is not true

Note that this is DISPROVING a UNIVERSAL statement by a counterexample

$\forall x\ \neg R(x)$, where R(x) means "x has red hair"

- Find one person (in the domain) who has red hair

Every positive integer is the square of another integer

- The square root of 5 is 2.236, which is not an integer