CSE 20
DISCRETE MATH

SPRING 2016

http://cseweb.ucsd.edu/classes/sp16/cse20-ac/

Today's learning goals

- Evaluate which proof technique(s) is appropriate for a given proposition
  - Direct proof
  - Proofs by contraposition
  - Proofs by contradiction
  - Proof by cases
  - Constructive existence proofs
- Correctly prove statements using appropriate style conventions, guiding text, notation, and terminology
- Define and differentiate between important sets
- Use correct notation when describing sets: {...}, intervals
- Define and prove properties of: subset relation, power set, Cartesian products of sets, union of sets, intersection of sets, disjoint sets, set differences, complement of a set

Overall proof strategy

- Do you believe the statement?
  - Try some small examples.
- Determine logical structure + main connective.
- Determine relevant definitions.
- Map out possible proof strategies.
  - For each strategy: what can we **assume**, what is the **goal**?
  - Start with simplest, move to more complicated if/when get stuck.

Main connective: conditional

Rosen p. 82

- Modus ponens **Direct proof**

To prove that "If P, then Q"

- Assume P is true.
- Use rules of inference, axioms, definitions to…
- … conclude Q is true.

Main connective: conditional

Rosen p. 83

- Modus tollens

Proof by contraposition

To prove that "If P, then Q"

- Assume Q is false.
- Use rules of inference, axioms, definitions to…
- … conclude P is also false.

Both modus ponens and modus tollens apply when proving a conditional statement

Universal conditionals

Rosen p. 88, 82

$$\forall n\ (\ldots \rightarrow \ldots)$$

To prove this statement is **false** :

Find a **counterexample**.

To prove this statement is **true** :

Select a **general element** of the domain, use rules of inference (e.g direct proof, proof by contrapositive, etc.) to prove that the conditional statement is true of this element, c conclude that it holds of all members of the domain.

Reminder: evens and odds

An integer a is **even** if there is some integer b such that

$$a = 2b$$

Which of the following is equivalent to definition of a being even?

A. a/2
B. a **div** 2 is an integer.
C. a **mod** 2 is zero.
D. 2a is an integer.
E. More than one of the above.

Reminder: evens and odds

An integer a is **even** if there is some integer b such that

$$a = 2b.$$

Why equivalent?

An integer a is **odd** iff

- it's not even

or equivalently

- there is some integer b such that

$$a = 2b + 1.$$

Flexing proof muscles

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

Proof:

Flexing proof muscles

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

Proof:

Let n be an arbitrary integer. Assume, towards a direct proof, that n is even. WTS that n^2 is also even. By definition of n being even, there is some integer c such that $n = 2c$. Squaring both sides, $n^2 = 4c^2$. Since c is an integer and integers are closed under multiplication, $2c^2$ is also an integer. Therefore, $x=2c^2$ serves as an example to prove the existential statement $\exists x(n^2 = 2x)$ which is the definition of n^2 being even, so the proof is complete.

Flexing proof muscles

Theorem: If n is odd, then so is n^2.

Proof:

Flexing proof muscles

Theorem: If n is odd, then so is n^2.

Proof:

Let n be an arbitrary integer. Assume, towards a direct proof, that n is odd. WTS that n^2 is also odd. By definition of n being odd, there is some integer c such that $n = 2c+1$. Squaring both sides, $n^2 = 4c^2+4c+1$. Since c is an integer and integers are closed under addition and multiplication, $2c^2+2c$ is also an integer. Since $n^2 = 2(2c^2+2c)+1$, $x = 2c^2+2c$ serves as an example to prove the existential statement which is the definition of n^2 being odd, so the proof is complete.

Flexing proof muscles

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

Proof:

Flexing proof muscles

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

Proof:

Let n be an arbitrary integer. Assume, towards a proof by contraposition, that that n is not even. WTS that n^2 is also not even. By definition of n, n is odd (since it's not even). Applying our previous theorem, we conclude that n^2 is also odd. By definition of odd, this means that n^2 is not even, as required.

Flexing proof muscles

Theorem: If n^2 is odd, then so is n.

Proof:

Flexing proof muscles

Theorem: If n^2 is odd, then so is n.

Proof:

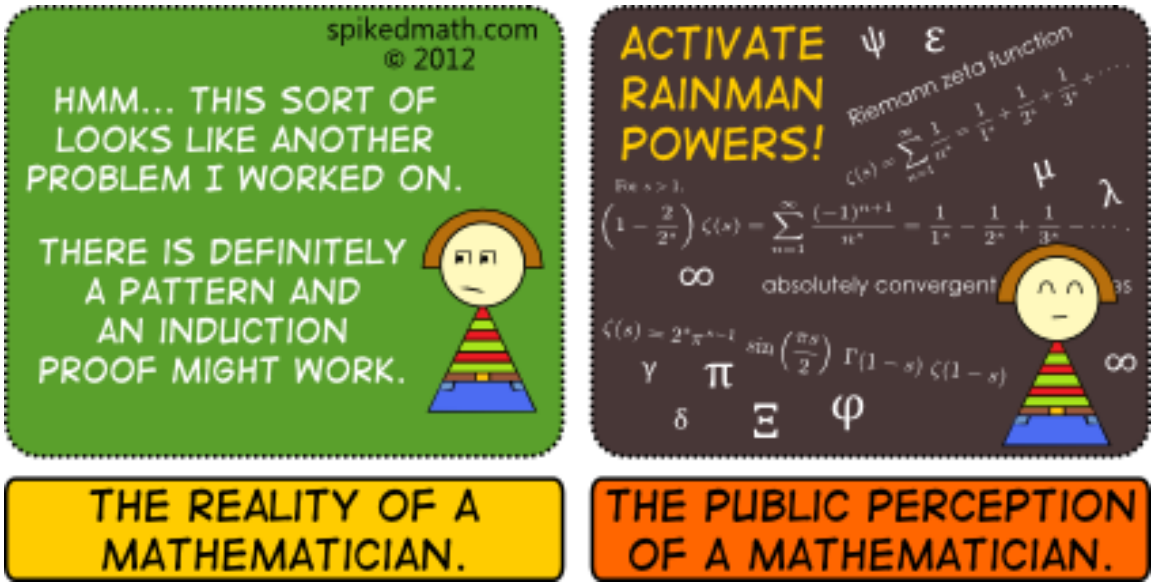
Let n be an arbitrary integer. Assume, towards a proof by contraposition, that that n is not odd. WTS that n^2 is also not odd. By definition of n, n is even (since it's not odd). Applying our previous theorem, we conclude that n^2 is also even. By definition of odd, this means that n^2 is not odd, as required.

Reminder: perfect squares

Rosen p. 83

Theorem: For integers k>1, then 2^k-1 is not a perfect square.

Proof: ???



Proof by contradiction

Rosen p. 86

Idea: To prove P, instead, we prove that the conditional

$$(\neg P) \rightarrow F$$

is true. **But**, the only way for a conditional to be true if its conclusion is false is for **its hypothesis to be false too**.

Conclude: $(\neg P)$ is false, i.e. **P is true**!

Back to: perfect squares

Rosen p. 83

Theorem: For integers k>1, then 2^k-1 is not a perfect square.

Proof:

What would we assume in a proof by contradiction?

A. k > 1
B. k <= 1
C. 2^k-1 is not a perfect square
D. 2^k-1 is a perfect square
E. More than one of the above

Back to: perfect squares *Rosen p. 83*

Theorem: For integers k>1, then 2^k-1 is not a perfect square.

Proof: Let k be an integer. Assume that

- k >1 **and that**
- 2^k-1 is a perfect square.

Goal: look for a contradiction that is now guaranteed.

Keep going …

Overall proof strategy

- Do you believe the statement?
  - Try some small examples.
- Determine logical structure + main connective.
- Determine relevant definitions.
- Map out possible proof strategies.

  Conditional statement? Direct OR contrapositive.
  Existential statement? Find an example.
  Universal statement? Start with generic element …
  Any statement: contradiction
  - For each strategy: what can we **assume**, what is the **goal**?
  - Start with simplest, move to more complicated if/when get stuck.

Some definitions

Rosen Sections 2.1, 2.2

Set: unordered collection of elements

"x is an element of set A"

$$x \in A$$

"x is **not** an element of set A"

$$x \notin A$$

Some definitions

Rosen Sections 2.1, 2.2

Set: unordered collection of **elements**

A = B iff $\forall x(x \in A \leftrightarrow x \in B)$

How to specify these elements?

- Roster $\{ \ldots \}$
- Set builder $\{x \in U \mid P(x)\}$

Some definitions

Rosen Sections 2.1, 2.2

Set: unordered collection of **elements**

A = B iff $\forall x(x \in A \leftrightarrow x \in B)$

Which of the following is not equal to the rest?

A. { 1, 2, 3 }

B. $\{\{1\},\{2\},\{3\}\}$

C. { 3, 1, 2 }

D. { 1, 1, 2, 3}

E. $\{x \in \mathbb{Z} \mid (x^2 - 4x + 3) = 0 \text{ or } x \text{ is an even prime}\}$

Some definitions

Rosen Sections 2.1, 2.2

Set: unordered **collection** of elements

Arrows in set builder notation indicate "and"

N: natural numbers {0, 1, 2, 3, …}

Z: integers {…, -2, -1, 0, 1, 2, …}

Z^+: positive integers {1, 2, 3, …}

Q: rational numbers $\{p/q \mid p \in \mathbb{Z}, q \in \mathbb{Z}, \text{ and } q \neq 0\}$

R: real numbers

R^+: positive real numbers

C: complex numbers

Some definitions

Rosen Sections 2.1, 2.2

Subset: $A \subseteq B$ means $\forall x(x \in A \rightarrow x \in B)$

Some definitions

Rosen Sections 2.1, 2.2

Subset: $A \subseteq B$ means $\forall x(x \in A \rightarrow x \in B)$

Theorem: For any sets A and B, A = B if and only if both $A \subseteq B$ and $B \subseteq A$

Proof:

What's the logical structure of this statement?

A. Universal conditional.
B. Biconditional.
C. Conjunction (and)
D. None of the above.

Some definitions

Rosen Sections 2.1, 2.2

Subset: $A \subseteq B$ means $\forall x(x \in A \rightarrow x \in B)$

Theorem: For any sets A and B, A = B if and only if both

$A \subseteq B$ and $B \subseteq A$

Proof: Let A and B be any sets.

- **WTS** if A=B, then both $A \subseteq B$ and $B \subseteq A$.
- **WTS** if both $A \subseteq B$ and $B \subseteq A$, then A=B.

Keep going …

Some definitions

Rosen Sections 2.1, 2.2

Subset: $A \subseteq B$ means $\forall x(x \in A \rightarrow x \in B)$

How would you prove that **R** is not a subset of **Q**?

A. Prove that every real number is not rational.
B. Prove that every rational number is real.
C. Prove that there is a real number that is rational.
D. Prove that there is a real number that is not rational.
E. Prove that there is a rational number that is not real.

An (ir)rational excursion

Rosen p. 86, 97

Theorem: R is not a subset of **Q**.

Lemma: $\sqrt{2}$ is not rational.

Corollary: There are irrational numbers x,y such that x^y is rational.

An (ir)rational excursion

Rosen p. 86, 97

Theorem: R is not a subset of **Q**.

What's the logical structure of each of these statements?

Lemma: $\sqrt{2}$ is not rational.

Recall: **Q**=$\{p/q \mid p \in \mathbb{Z}, q \in \mathbb{Z}, \text{ and } q \neq 0\}$

Details of proof in page 86: use contradiction!

Corollary: There are irrational numbers x,y such that x^y is rational.

Existential statement: can we build a witness?

An (ir)rational excursion

Rosen p. 86, 97

Theorem: R is not a subset of **Q**.

What's the logical structure of each of these statements?

Lemma: $\sqrt{2}$ is not rational.

Corollary: There are irrational numbers x,y such that x^y is rational.

Some definitions

Rosen Sections 2.1, 2.2

Empty set: $\emptyset = \{\} = \{x : x \neq x\}$

Which of the following is not equal to the rest?

A. $\{\}$

B. $\{\emptyset\}$

C. $\emptyset$

D. $\{x \in \mathbb{Z} \mid x > x^2\}$

E. $\{x \mid x \in \emptyset\}$

Some definitions

Rosen Sections 2.1, 2.2

Power set: For a set S, its powers set is the set of all subsets of S. $\mathcal{P}(S) = \{A \mid A \subseteq S\}$

Which of the following is **not** true (in general)?

A. $S \in \mathcal{P}(S)$

B. $\emptyset \in \mathcal{P}(S)$

C. $S \subseteq \mathcal{P}(S)$

D. $\emptyset \subseteq \mathcal{P}(S)$

E. $\emptyset \in S$