INFORMATION & COMPUTER SCIENCES
UNIVERSITY of HAWAI'I at MĀNOA

Ch 1.7: Introduction to Proofs

ICS 141: Discrete Mathematics for Computer Science I

KYLE BERNEY
DEPARTMENT OF ICS, UNIVERSITY OF HAWAII AT MANOA

Proofs

- A proof is a valid argument that establishes the truth of a mathematical statement
- To construct a proof, we can use:
  - Hypotheses of the statement
  - Axioms (fundamental statements we assume to be true)
  - Previously proven statements

Proof Writing Conventions

- Proofs are written using first person plural
  - Tradition
  - Suggests a collaborative reasoning between the reader and writer

Proof Writing Conventions

- Proofs are written using first person plural
  - Tradition
  - Suggests a collaborative reasoning between the reader and writer
- Common phrases:

1. Starting a train of thought
   - “Assume that ...”
   - “We begin by ...”
   - “Let us consider ...”
   - “We are given that ...”
   - “Suppose that ...”

Proof Writing Conventions

- Proofs are written using first person plural
  - Tradition
  - Suggests a collaborative reasoning between the reader and writer
- Common phrases:

  2. Making Observations
     - “We observe that ...”
     - “Notice that ...”
     - “We see that ...”
     - “We note that ...”

Proof Writing Conventions

- Proofs are written using first person plural
  - Tradition
  - Suggests a collaborative reasoning between the reader and writer
- Common phrases:

  3. Applying definitions or known results
     - "By definition ..."
     - "From Theorem ..., we know that ..."
     - "We use the fact that ..."
     - "Recall that ..."

Proof Writing Conventions

- Proofs are written using first person plural
  - Tradition
  - Suggests a collaborative reasoning between the reader and writer
- Common phrases:

  4. Concluding the proof
     - “We have shown that ...”
     - “Therefore, ...”

Proof Writing Conventions

- At the end of a proof we write ■ or □ (tombstone symbols)
  - Tradition
  - Formality
  - Clarity
- Historically, “Q.E.D.” was used
  - Latin phrase, “Quod Erat Demonstrandum”
  - Translates to “that which was to be demonstrated” or “what was to be shown”

Terminology

- Different terms are used to describe various mathematical statements, generally based on the importance or use

Terminology

- Different terms are used to describe various mathematical statements, generally based on the importance or use
  - A <u>theorem</u> is a statement that can be proven and often represents a significant result

Terminology

- Different terms are used to describe various mathematical statements, generally based on the importance or use
  - A theorem is a statement that can be proven and often represents a significant result
  - A proposition is statement that can be proven and is less significant than a theorem, but is still of interest

Terminology

- Different terms are used to describe various mathematical statements, generally based on the importance or use
  - A <u>theorem</u> is a statement that can be proven and often represents a significant result
  - A <u>proposition</u> is statement that can be proven and is less significant than a theorem, but is still of interest
  - A <u>lemma</u> is a preliminary result that can be proven and assists in proving a proposition or theorem

Terminology

- Different terms are used to describe various mathematical statements, generally based on the importance or use
  - A theorem is a statement that can be proven and often represents a significant result
  - A proposition is statement that can be proven and is less significant than a theorem, but is still of interest
  - A lemma is a preliminary result that can be proven and assists in proving a proposition or theorem
  - A corollary is a result that follows directly from a theorem or another proven statement

Terminology

- Different terms are used to describe various mathematical statements, generally based on the importance or use
  - A theorem is a statement that can be proven and often represents a significant result
  - A proposition is statement that can be proven and is less significant than a theorem, but is still of interest
  - A lemma is a preliminary result that can be proven and assists in proving a proposition or theorem
  - A corollary is a result that follows directly from a theorem or another proven statement
  - A conjecture is a statement that is being proposed as a true statement based on evidence or intuition

Direct Proofs

- A direct proof is a method of proving a mathematical statement by following a sequence of logical steps that follows directly from the assumptions to the statement being proven.

Direct Proofs

- A direct proof is a method of proving a mathematical statement by following a sequence of logical steps that follows directly from the assumptions to the statement being proven.

- To prove a conditional statement $P \Rightarrow Q$

  1. Assume the hypothesis, P, is true
  2. Use definitions, axioms, and other previously proven results to duduce further statements
  3. Conclude that the conclusion, Q, is true based on the previous logical steps

Even and Odd Integers

- Definition: An integer n is even if there exists an integer k such that
$$n = 2k \ .$$
- Definition: An integer n is odd if there exists an integer k such that
$$n = 2k + 1 \ .$$

Even and Odd Integers

- Definition: An integer n is even if there exists an integer k such that

$$n = 2k\ .$$

- Definition: An integer n is odd if there exists an integer k such that

$$n = 2k + 1\ .$$

- *Note:*
  - Every integer is either even or odd
  - No integer is both even and odd

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.
  - $\forall n(P(n) \Rightarrow Q(n))$
  - $P(n)$ = "n is an odd integer"
  - $Q(n)$ = "n^2 is odd"

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.
  - $\forall n(P(n) \Rightarrow Q(n))$
  - $P(n)$ = "n is an odd integer"
  - $Q(n)$ = "n^2 is odd"

- Proof Sketch:

1. Assume $P(n)$ is true
   - Let n be an arbitrary odd integer

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.
  - $\forall n(P(n) \Rightarrow Q(n))$
  - $P(n)$ = "n is an odd integer"
  - $Q(n)$ = "n^2 is odd"

- Proof Sketch:

1. Assume $P(n)$ is true
   - Let n be an arbitrary odd integer

- *Note:*
  - It is important that the value of n is arbitrary to ensure that the proof applies to all values of n (rather than a specific value of n)

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.
  - $\forall n(P(n) \Rightarrow Q(n))$
  - $P(n)$ = "n is an odd integer"
  - $Q(n)$ = "n^2 is odd"

- Proof Sketch:

2. Use definitions, axioms, and other previously proven results to duduce further statements
   - By definition of an odd integer, there exists an integer k such that

$$n = 2k + 1$$

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.
  - $\forall n(P(n) \Rightarrow Q(n))$
  - $P(n)$ = "n is an odd integer"
  - $Q(n)$ = "n^2 is odd"

- Proof Sketch:

2. Use definitions, axioms, and other previously proven results to duduce further statements
   - Use algebra to deduce the value of n^2

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1\ . \end{aligned}$$

Direct Proofs

- <u>Proposition:</u> If n is an odd integer, then n^2 is odd.
  - $\forall n(P(n) \Rightarrow Q(n))$
  - $P(n)$ = "n is an odd integer"
  - $Q(n)$ = "n^2 is odd"

- <u>Proof Sketch:</u>

  2. Use definitions, axioms, and other previously proven results to duduce further statements
     - For clarity, we define a new integer $k' = 2k^2 + 2k$

$$n^2 = 2(2k^2 + 2k) + 1$$
$$= 2k' + 1 \ .$$

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.
  - $\forall n(P(n) \Rightarrow Q(n))$
  - $P(n)$ = "n is an odd integer"
  - $Q(n)$ = "n^2 is odd"
- Proof Sketch:
  3. Conclude that the $Q(n)$ is true based on the previous logical steps
     - We showed that there exists an integer $k' = 2k^2 + 2k$ such that $n^2 = 2k' + 1$
     - By definition of an odd integer, n^2 is odd

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.
- Proof:

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.
- Proof: Let n be an arbitrary odd integer.

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.

- Proof: Let n be an arbitrary odd integer. By definition of an odd integer, there exists an integer k such that $n = 2k + 1$.

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.
- Proof: Let n be an arbitrary odd integer. By definition of an odd integer, there exists an integer k such that $n = 2k + 1$. Hence, we have that

$$
\begin{aligned}
n^2 &= (2k+1)^2 \\
&= 4k^2 + 4k + 1 \\
&= 2(2k^2 + 2k) + 1 \\
&= 2k' + 1, \text{ for } k' = 2k^2 + 2k\ .
\end{aligned}
$$

Direct Proofs

- Proposition: If n is an odd integer, then n^2 is odd.

- Proof: Let n be an arbitrary odd integer. By definition of an odd integer, there exists an integer k such that $n = 2k + 1$. Hence, we have that

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \\ &= 2k' + 1, \text{ for } k' = 2k^2 + 2k\ . \end{aligned}$$

Since $k' = 2k^2 + 2k$ is an integer, by definiton of an odd integer n^2 is odd. ■

Direct Proofs

- Definition: An integer a is a perfect square if there is an integer b such that $a = b^2$.

Direct Proofs

- Proposition: If m and n are both perfect squares, then nm is also a perfect square.

Direct Proofs

- Proposition: If m and n are both perfect squares, then nm is also a perfect square.
- Proof:

Direct Proofs

- Proposition: If m and n are both perfect squares, then nm is also a perfect square.

- Proof: Let m and n be arbitrary integers such that $m = x^2$ and $n = y^2$ for some integers x and y.

Direct Proofs

- Proposition: If m and n are both perfect squares, then nm is also a perfect square.
- Proof: Let m and n be arbitrary integers such that $m = x^2$ and $n = y^2$ for some integers x and y.

$$
\begin{aligned}
mn &= x^2y^2 \\
&= (xx)(yy) \\
&= (xy)(xy) \\
&= (xy)^2 \\
&= z^2, \text{ for } z = xy\ .
\end{aligned}
$$

Direct Proofs

- Proposition: If m and n are both perfect squares, then nm is also a perfect square.

- Proof: Let m and n be arbitrary integers such that $m = x^2$ and $n = y^2$ for some integers x and y.

$$\begin{aligned} mn &= x^2 y^2 \\ &= (xx)(yy) \\ &= (xy)(xy) \\ &= (xy)^2 \\ &= z^2, \text{ for } z = xy\ . \end{aligned}$$

It follows from the definition of a perfect square that mn is also a perfect square. ■

Direct Proofs

- <u>Conjecture:</u>

$$0.999\overline{9} = 1$$

- True or False?

Direct Proofs

- Proposition:

$$0.999\overline{9} = 1$$

- Proof:

Direct Proofs

- Proposition:

$$0.999\overline{9} = 1$$

- Proof: Let $x = 0.999\overline{9}$

Direct Proofs

- <u>Proposition:</u>

$$0.999\overline{9} = 1$$

- <u>Proof:</u>

$$\text{Let } x = 0.999\overline{9}$$

$$\Leftrightarrow 10x = 9.999\overline{9}$$

Direct Proofs

- <u>Proposition:</u>

$$0.999\overline{9} = 1$$

- <u>Proof:</u>

$$\begin{aligned} \text{Let } x &= 0.999\overline{9} \\ \Leftrightarrow 10x &= 9.999\overline{9} \\ &= 9 + 0.999\overline{9} \end{aligned}$$

Direct Proofs

- Proposition:

$$0.999\overline{9} = 1$$

- Proof:

$$\begin{aligned} \text{Let } x &= 0.999\overline{9} \\ \Leftrightarrow 10x &= 9.999\overline{9} \\ &= 9 + 0.999\overline{9} \\ &= 9 + x \end{aligned}$$

Direct Proofs

- Proposition:

$$0.999\overline{9} = 1$$

- Proof:

$$\begin{aligned} \text{Let } x &= 0.999\overline{9} \\ \Leftrightarrow 10x &= 9.999\overline{9} \\ &= 9 + 0.999\overline{9} \\ &= 9 + x \\ \Leftrightarrow 9x &= 9 \end{aligned}$$

Direct Proofs

- Proposition:

$$0.999\overline{9} = 1$$

- Proof:

$$\begin{aligned} \text{Let } x &= 0.999\overline{9} \\ \Leftrightarrow 10x &= 9.999\overline{9} \\ &= 9 + 0.999\overline{9} \\ &= 9 + x \\ \Leftrightarrow 9x &= 9 \\ \Leftrightarrow x &= 1\,. \quad \blacksquare \end{aligned}$$

Proof by Contraposition

- Recall that a conditional statement $P \Rightarrow Q$ is logically equivalent to its contrapositive $\neg Q \Rightarrow \neg P$

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

- We can use this logical equivalence to construct a proof by contraposition.

Proof by Contraposition

- Recall that a conditional statement $P \Rightarrow Q$ is logically equivalent to its contrapositive $\neg Q \Rightarrow \neg P$

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

- We can use this logical equivalence to construct a proof by contraposition.

Proof by Contraposition

- To prove a conditional statement $P \Rightarrow Q$ via its contrapositive $\neg Q \Rightarrow \neg P$

1. Assume the negation of the conclusion, $\neg Q$, is true
2. Use definitions, axioms, and other previously proven results to duduce further statements
3. Conclude that the negation of the hypothesis, $\neg P$, is true based on the previous logical steps

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.

- Proof Sketch: (Direct proof)

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.
- Proof Sketch: (Direct proof)

$$3n + 2 = 2k + 1, \text{ for some integer } k$$

$$\Leftrightarrow 3n = 2k - 1$$

$$\Leftrightarrow n = \frac{2k - 1}{3}.$$

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.
- Proof Sketch: (Direct proof)

$$3n + 2 = 2k + 1, \text{ for some integer } k$$
$$\Leftrightarrow 3n = 2k - 1$$
$$\Leftrightarrow n = \frac{2k - 1}{3}.$$

- There does not seem to be any direct way to conclude that n is odd.

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.
  - $\forall n(\neg Q(n) \Rightarrow \neg P(n))$
  - $\neg Q(n)$ = "n is even"
  - $\neg P(n)$ = "$3n + 2$ is even"
- Proof Sketch: (Proof by contraposition)

Proof by Contraposition

- Proposition: If n is an integer and $3n+2$ is odd, then n is odd.
  - $\forall n(\neg Q(n) \Rightarrow \neg P(n))$
  - $\neg Q(n)$ = "n is even"
  - $\neg P(n)$ = "$3n+2$ is even"
- Proof Sketch: (Proof by contraposition)

1. Assume the negation of the conclusion, $\neg Q(n)$, is true
   - Let n be an arbitrary even integer

Proof by Contraposition

- <u>Proposition:</u> If n is an integer and $3n + 2$ is odd, then n is odd.
  - $\forall n(\neg Q(n) \Rightarrow \neg P(n))$
  - $\neg Q(n)$ = "n is even"
  - $\neg P(n)$ = "$3n + 2$ is even"
- <u>Proof Sketch:</u> (Proof by contraposition)

2. Use definitions, axioms, and other previously proven results to duduce further statements
   - By definition of an even integer, there exists an integer k such that

$$n = 2k$$

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.
  - $\forall n(\neg Q(n) \Rightarrow \neg P(n))$
  - $\neg Q(n)$ = "n is even"
  - $\neg P(n)$ = "$3n + 2$ is even"
- Proof Sketch: (Proof by contraposition)

2. Use definitions, axioms, and other previously proven results to duduce further statements
   - Use algebra to deduce the value of $3n + 2$

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1) \\ &= 2k', \text{ for } k' = 3k + 1 \ . \end{aligned}$$

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.
  - $\forall n(\neg Q(n) \Rightarrow \neg P(n))$
  - $\neg Q(n)$ = "n is even"
  - $\neg P(n)$ = "$3n + 2$ is even"
- Proof Sketch: (Proof by contraposition)

3. Conclude that the negation of the hypothesis, $\neg P(n)$, is true based on the previous logical steps
   - We showed that $3n + 2 = 2k'$ for integer $k' = 3k + 1$
   - By definition of an even integer, $3n + 2$ is even

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.

- Proof: We proceed by proof by contraposition.

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.
- Proof: We proceed by proof by contraposition. Let n be an arbitrary even integer such that $n = 2k$ for some integer k.

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.

- Proof: We proceed by proof by contraposition. Let n be an arbitrary even integer such that $n = 2k$ for some integer k.

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1) \\ &= 2k', \text{ for } k' = 3k + 1\ . \end{aligned}$$

Proof by Contraposition

- Proposition: If n is an integer and $3n+2$ is odd, then n is odd.

- Proof: We proceed by proof by contraposition. Let n be an arbitrary even integer such that $n = 2k$ for some integer k.

$$\begin{aligned} 3n+2 &= 3(2k)+2 \\ &= 6k+2 \\ &= 2(3k+1) \\ &= 2k', \text{ for } k' = 3k+1 \ . \end{aligned}$$

Since $3n+2 = 2k'$ for integer $k' = 3k+1$, by definition of an even integer $3n+2$ is even.

Proof by Contraposition

- Proposition: If n is an integer and $3n + 2$ is odd, then n is odd.

- Proof: We proceed by proof by contraposition. Let n be an arbitrary even integer such that $n = 2k$ for some integer k.

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1) \\ &= 2k', \text{ for } k' = 3k + 1 \ . \end{aligned}$$

  Since $3n + 2 = 2k'$ for integer $k' = 3k + 1$, by definition of an even integer $3n + 2$ is even. We have shown that the contrapositive is true, therefore, if $3n + 2$ is odd then n is odd is also true. ■

Exercise

- Lemma: For any positive real numbers s, t, u and v, if $s < t$ and $u < v$ then $su < tv$.

Exercise

- Lemma: For any positive real numbers s, t, u and v, if $s < t$ and $u < v$ then $su < tv$.
- *Hint #1:* Try a direct proof

Exercise

- Lemma: For any positive real numbers s, t, u and v, if $s < t$ and $u < v$ then $su < tv$.

- *Hint #1:* Try a direct proof
- *Hint #2:* Remember that multiplying inequalities by positive numbers do not affect the direction of the inequality

Exercise

- Lemma: For any positive real numbers s, t, u and v, if $s < t$ and $u < v$ then $su < tv$.
- Proof:

Exercise

- Lemma: For any positive real numbers s, t, u and v, if $s < t$ and $u < v$ then $su < tv$.
- Proof: Let s, t, u, and v be arbitrary positive such that $s < t$ and $u < v$.

Exercise

- Lemma: For any positive real numbers s, t, u and v, if $s < t$ and $u < v$ then $su < tv$.
- Proof: Let s, t, u, and v be arbitrary positive real numbers such that $s < t$ and $u < v$. Since $s < t$ and u is positive, $su < tu$.

Exercise

- Lemma: For any positive real numbers s, t, u and v, if $s < t$ and $u < v$ then $su < tv$.
- Proof: Let s, t, u, and v be arbitrary positive real numbers such that $s < t$ and $u < v$. Since $s < t$ and u is positive, $su < tu$. Similarly since $u < v$ and t is positive, $ut < vt$.

Exercise

- Lemma: For any positive real numbers s, t, u and v, if $s < t$ and $u < v$ then $su < tv$.
- Proof: Let s, t, u, and v be arbitrary positive real numbers such that $s < t$ and $u < v$. Since $s < t$ and u is positive, $su < tu$. Similarly since $u < v$ and t is positive, $tu < tv$. Therefore, $su < tu < tv$. ■

Proof by Contraposition

- Proposition: If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof by Contraposition

- Proposition: If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
- Proof: We proceed with proof by contraposition.

Proof by Contraposition

- Proposition: If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

- Proof: We proceed with proof by contraposition.

  1. Assume the negation of the conclusion, $\neg Q(n)$, is true
     - Using De Morgan's law,

$$a > \sqrt{n} \text{ and } b > \sqrt{n}$$

Proof by Contraposition

- Proposition: If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
- Proof: We proceed with proof by contraposition. Let a and b be arbitrary positive integers and $n = ab$. Assume that $a > \sqrt{n}$ and $b > \sqrt{n}$.

Proof by Contraposition

- Proposition: If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
- Proof: We proceed with proof by contraposition. Let a and b be arbitrary positive integers and $n = ab$. Assume that $a > \sqrt{n}$ and $b > \sqrt{n}$. From the previous Lemma (Slide 16), we know that if $0 < s < t$ and $0 < u < v$ then $su < tv$.

Proof by Contraposition

- Proposition: If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
- Proof: We proceed with proof by contraposition. Let a and b be arbitrary positive integers and $n = ab$. Assume that $a > \sqrt{n}$ and $b > \sqrt{n}$. From the previous Lemma (Slide 16), we know that if $0 < s < t$ and $0 < u < v$ then $su < tv$. Hence, $ab > (\sqrt{n})(\sqrt{n}) = n$ and $ab \neq n$. ■

Vacuous Proof

- Recall that a conditional statement $P \Rightarrow Q$ is always true if P is false.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Vacuous Proof

- Recall that a conditional statement $P \Rightarrow Q$ is always true if P is false.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

- A vacuous proof shows that P is false
  - Often used to establish special cases of statements
  - Base case(s) in proof by induction (Chapter 5)

Vacuous Proof

- Proposition: If n is an integer such that n is a perfect square and $10 \leq n \leq 15$, then n is also a perfect cube.

Vacuous Proof

- Proposition: If n is an integer such that n is a perfect square and $10 \leq n \leq 15$, then n is also a perfect cube.

- Proof: There does not exist a value for n that is a perfect square and between the values of 10 and 15. Therefore, the proposition is vacuously true. ■

Trivial Proof

- Recall that a conditional statement $P \Rightarrow Q$ is always true if Q is true.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Trivial Proof

- Recall that a conditional statement $P \Rightarrow Q$ is always true if Q is true.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

- A trivial proof shows that Q is true
  - Often used to establish special cases of statements
  - Base case(s) in proof by induction (Chapter 5)

"Trivial" Proof

- A trivial proof may also refer to an "easy" proof
- Whether a proof or "easy" or not depends on the person constructing the proof!
  - An expert may consider a proof trivial
  - A novice may consider the proof non-trivial
- Common (math) joke to say that any proof is trivial, as long as you know how to prove it.
- In this class, we will construct our proofs assuming everyone is a novice
  - In general, this is what you should assume, as you never know who is going to be reading your proofs

Trivial Proof

- Proposition: Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$", where the domain is all non-negative integers. Show that $P(0)$ is true.

Trivial Proof

- Proposition: Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$", where the domain is all non-negative integers. Show that $P(0)$ is true.

- Proof: We evaluate $P(0)$ which results in $a^0 = b^0 = 1$. Therefore, $P(0)$ is trivially true. ■

Proof by Contradiction

- A proof by contradiction proves that a proposition $P \Rightarrow Q$ is true by:

  1. Assume that the negation of the proposition $\neg(P \Rightarrow Q)$ is true
  2. Show that $\neg(P \Rightarrow Q)$ leads to a contradiction, hence $\neg(P \Rightarrow Q)$ must be false
  3. It follows that $\neg(P \Rightarrow Q) \Rightarrow \mathrm{F}$ is true and therefore $P \Rightarrow Q$ is also true

Proof by Contradiction

- A proof by contradiction proves that a proposition $P \Rightarrow Q$ is true by:
  1. Assume that the negation of the proposition $\neg(P \Rightarrow Q)$ is true
  2. Show that $\neg(P \Rightarrow Q)$ leads to a contradiction, hence $\neg(P \Rightarrow Q)$ must be false
  3. It follows that $\neg(P \Rightarrow Q) \Rightarrow \mathrm{F}$ is true and therefore $P \Rightarrow Q$ is also true
- *Note:*

$$\begin{aligned} \neg(P \Rightarrow Q) &\equiv \neg(\neg P \vee Q) \\ &\equiv P \wedge \neg Q\,. \end{aligned}$$

Proof by Contradiction

- A <u>proof by contradiction</u> proves that a proposition $P \Rightarrow Q$ is true by:
  1. Assume that the negation of the proposition $\neg(P \Rightarrow Q)$ is true
  2. Show that $\neg(P \Rightarrow Q)$ leads to a contradiction, hence $\neg(P \Rightarrow Q)$ must be false
  3. It follows that $\neg(P \Rightarrow Q) \Rightarrow$ F is true and therefore $P \Rightarrow Q$ is also true

P	Q	$P \Rightarrow Q$	$\neg Q$	$P \wedge \neg Q$	F	$(P \wedge \neg Q) \Rightarrow$ F
T	T	T	F	F	F	T
T	F	F	T	T	F	F
F	T	T	F	F	F	T
F	F	T	T	F	F	T

Rational and Irrational Numbers

- Definition: A real number r is rational if there exists integers p and q with $q \neq 0$ such that
$$r = \frac{p}{q}.$$
- Definition: A real number r is irrational if it is not rational.

Proof by Contradiction

- Proposition: $\sqrt{2}$ is irrational.
- Proof Sketch:

Proof by Contradiction

- Proposition: $\sqrt{2}$ is irrational.
- Proof Sketch:

1. Assume the negation of the proposition ($\neg P$) is true
    - Assume for the sake of contradiction that $\sqrt{2}$ is rational.

Proof by Contradiction

- Proposition: $\sqrt{2}$ is irrational.

- Proof Sketch:

2. Show that $\neg P$ leads to a contradiction
   - By definition of a rational number, there exists integers a and b, where $b \neq 0$ and a and b have no common factors, such that

$$\sqrt{2} = \frac{a}{b}$$

Proof by Contradiction

- Proposition: $\sqrt{2}$ is irrational.

- Proof Sketch:

2. Show that $\neg P$ leads to a contradiction
   - By definition of a rational number, there exists integers a and b, where $b \neq 0$ and a and b have no common factors, such that

$$\sqrt{2} = \frac{a}{b}$$
$$\Rightarrow 2 = \frac{a^2}{b^2}$$
$$\Rightarrow 2b^2 = a^2 .$$

Proof by Contradiction

- Proposition: $\sqrt{2}$ is irrational.
- Proof Sketch:

2. Show that $\neg P$ leads to a contradiction
    - By definition of an even integer, it follows that a^2 is even.
    - From Exercise 18 (in textbook), if a^2 is even then a is also even.
    - By definition of an even integer, there exists an integer c such that $a = 2c$.

Proof by Contradiction

- Proposition: $\sqrt{2}$ is irrational.

- Proof Sketch:

2. Show that $\neg P$ leads to a contradiction
   - By definition of an even integer, it follows that a^2 is even.
   - From Exercise 18 (in textbook), if a^2 is even then a is also even.
   - By definition of an even integer, there exists an integer c such that $a = 2c$.

$$\begin{aligned} 2b^2 &= a^2 \\ &= (2c)^2 \\ &= 4c^2 \\ \Leftrightarrow b^2 &= 2c^2 . \end{aligned}$$

Proof by Contradiction

- Proposition: $\sqrt{2}$ is irrational.

- Proof Sketch:

2. Show that $\neg P$ leads to a contradiction
   - Since $b^2 = 2c^2$, by definition b^2 is even.
   - From Exercise 18 (in textbook), if b^2 is even then b is also even.

Proof by Contradiction

- Proposition: $\sqrt{2}$ is irrational.
- Proof Sketch:

2. Show that $\neg P$ leads to a contradiction
   - We showed that both a and b are even, hence, they both have a common factor of 2
   - However, we assumed that a and b have no common factors, a contradiction.

Proof by Contradiction

- Proposition: $\sqrt{2}$ is irrational.

- Proof Sketch:

3. It follows that P is also true
    - Therefore, $\sqrt{2}$ is irrational

Proof by Contradiction

- Proposition: For an integer n, if $3n + 2$ is odd then n is odd.

Proof by Contradiction

- Proposition: For an integer n, if $3n + 2$ is odd then n is odd.

- Proof:

  1. Assume that the negation of the proposition $\neg(P \Rightarrow Q) \equiv (P \wedge \neg Q)$ is true
     - $3n + 2$ is odd
     - n is even

Proof by Contradiction

- Proposition: For an integer n, if $3n + 2$ is odd then n is odd.

- Proof: Let n be an arbitrary integer. Assume for the sake of contradiction that $3n + 2$ is odd and n is even.

Proof by Contradiction

- Proposition: For an integer n, if $3n + 2$ is odd then n is odd.

- Proof: Let n be an arbitrary integer. Assume for the sake of contradiction that $3n + 2$ is odd and n is even. By definition of an even integer, there exists an integer k such that $n = 2k$.

Proof by Contradiction

- Proposition: For an integer n, if $3n + 2$ is odd then n is odd.

- Proof: Let n be an arbitrary integer. Assume for the sake of contradiction that $3n + 2$ is odd and n is even. By definition of an even integer, there exists an integer k such that $n = 2k$.

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1) \\ &= 2k' \text{ for } k' = 3k + 1 \ . \end{aligned}$$

Proof by Contradiction

- Proposition: For an integer n, if $3n + 2$ is odd then n is odd.
- Proof: Let n be an arbitrary integer. Assume for the sake of contradiction that $3n + 2$ is odd and n is even. By definition of an even integer, there exists an integer k such that $n = 2k$.

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1) \\ &= 2k' \text{ for } k' = 3k + 1 \ . \end{aligned}$$

By definition, $3n + 2$ is also even, a contradiction.

Proof by Contradiction

- Proposition: For an integer n, if $3n+2$ is odd then n is odd.

- Proof: Let n be an arbitrary integer. Assume for the sake of contradiction that $3n+2$ is odd and n is even. By definition of an even integer, there exists an integer k such that $n = 2k$.

$$\begin{aligned} 3n+2 &= 3(2k)+2 \\ &= 6k+2 \\ &= 2(3k+1) \\ &= 2k' \text{ for } k' = 3k+1 \;. \end{aligned}$$

By definition, $3n+2$ is also even, a contradiction. Therefore, if $3n+2$ is odd then n is odd. ■

Proofs of Equivalance

- To prove a proposition that is a biconditional statement ($P \Leftrightarrow Q$), prove both:
  - $P \Rightarrow Q$
  - $Q \Rightarrow P$

Exercises

- Proposition: Let m, n, and p be integers. If $m + n$ and $n + p$ are even integers, then $m + p$ is even.

Exercises

- Proposition: Prove that every odd integer is the difference of two squares.

Exercises

- Proposition: Use a proof by contradiction to prove that the sum of an irrational number and a rational number is irrational.

Exercises

- Proposition: If x is irrational, then $\frac{1}{x}$ is irrational.

Exercises

- Proposition: If x is an irrational number and $x > 0$, then $\sqrt{x}$ is also irrational.

Exercises

- Proposition: Let n be an integer. If $n^3 + 5$ is odd, then n is even.

Exercises

- Proposition: Prove the proposition $P(0)$, where $P(n)$ is the proposition "If n is a positive integer greater than 1, then $n^2 > n$."

Exercises

- Proposition: Let n be a positive integer. n is odd if and only if $5n + 6$ is odd.