COMP170
Discrete Mathematical Tools for Computer Science

Lecture 9

Version 2: Last updated, Oct 25, 2005

Discrete Math for Computer Science
K. Bogart, C. Stein and R.L. Drysdale
Section 3.3, pp. 117-124

3.3 Inference

- What is a Proof?
- Direct Inference (Modus Ponens)
- Rules of Inference for Direct Proofs
- Contrapositive Rule of Inference
- Proof by Contradiction

What is a *Mathematical Proof*, really?

What is a *Mathematical Proof*, really?

- In this section we will introduce various techniques used to develop mathematical proofs.

What is a *Mathematical Proof*, really?

- In this section we will introduce various techniques used to develop mathematical proofs.

  Some of these techniques will actually be variations on similar ideas (so don't get confused if they look similar to each other).

What is a *Mathematical Proof*, really?

- In this section we will introduce various techniques used to develop mathematical proofs.

  Some of these techniques will actually be variations on similar ideas (so don't get confused if they look similar to each other).

- We start by examining a simple mathematical proof and its components

Prove that if m is even, then m^2 is even.

Prove that if m is even, then m^2 is even.

Let m be an integer.

Prove that if m is even, then m^2 is even.

Let m be an integer.

Suppose that m is even.

Prove that if m is even, then m^2 is even.

Let m be an integer.

Suppose that m is even.

If m is even, then $\exists k$ with $m = 2k$.

Prove that if m is even, then m^2 is even.

Let m be an integer.

Suppose that m is even.

If m is even, then $\exists k$ with $m = 2k$.

Then $\exists k$ such that $m = 2k$.

Prove that if m is even, then m^2 is even.

Let m be an integer.

Suppose that m is even.

If m is even, then $\exists k$ with $m = 2k$.

Then $\exists k$ such that $m = 2k$.

Then $\exists k$ such that $m^2 = 4k^2$.

Prove that if m is even, then m^2 is even.

Let m be an integer.

Suppose that m is even.

If m is even, then $\exists k$ with $m = 2k$.

Then $\exists k$ such that $m = 2k$.

Then $\exists k$ such that $m^2 = 4k^2$.

Then, there is an integer $h = 2k^2$ s.t. $m^2 = 2h$.

Prove that if m is even, then m^2 is even.

Let m be an integer.

Suppose that m is even.

If m is even, then $\exists k$ with $m = 2k$.

Then $\exists k$ such that $m = 2k$.

Then $\exists k$ such that $m^2 = 4k^2$.

Then, there is an integer $h = 2k^2$ s.t. $m^2 = 2h$.

Thus, if m is even, then m^2 is even.

3.3 Inference

- What is a Proof?
- Direct Inference (Modus Ponens)
- Rules of Inference for Direct Proofs
- Contrapositive Rule of Inference
- Proof by Contradiction

Consider the statements

1) Suppose that m is even.
2) If m is even, then $\exists k$ with $m = 2k$.
3) Then $\exists k$ such that $m = 2k$.

Consider the statements

1) Suppose that m is even.

2) If m is even, then $\exists k$ with $m = 2k$.

3) Then $\exists k$ such that $m = 2k$.

Let $p \sim (m \text{ is even})$ and $q \sim (\exists k \text{ with } m = 2k)$

Consider the statements

1) Suppose that m is even.

2) If m is even, then $\exists k$ with $m = 2k$.

3) Then $\exists k$ such that $m = 2k$.

Let $p \sim (m \text{ is even})$ and $q \sim (\exists k \text{ with } m = 2k)$

Then we can rewrite the three statements as

Consider the statements

1) Suppose that m is even.

2) If m is even, then $\exists k$ with $m = 2k$.

3) Then $\exists k$ such that $m = 2k$.

Let $p \sim$ (m is even) and $q \sim$ ($\exists k$ with $m = 2k$)

Then we can rewrite the three statements as

1) p

2) If p then q $\quad (p \Rightarrow q)$

3) q

Direct Inference (Modus Ponens)

Direct Inference (Modus Ponens)

Principle 3.3 (Direct inference)
From p and $p \Rightarrow q$ we may conclude q.

Direct Inference (Modus Ponens)

Principle 3.3 (Direct inference)
From p and $p \Rightarrow q$ we may conclude q.

Why is this valid?

Direct Inference (Modus Ponens)

Principle 3.3 (Direct inference)
From p and $p \Rightarrow q$ we may conclude q.

Why is this valid?

IMPLIES

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

In our example proof we showed that

If m is even then m^2 is even.

Essentially, we assumed m is even and derived that m^2 is even.

In symbols, we showed that

$(m \text{ is even}) \Rightarrow (m^2 \text{ is even})$.

In our example proof we showed that

If m is even then m^2 is even.

Essentially, we assumed m is even
and derived that m^2 is even.

In symbols, we showed that
$(m \text{ is even}) \Rightarrow (m^2 \text{ is even})$.

Principle 3.4 (Conditional Proof)
If by assuming p we may prove q, then the statement $p \Rightarrow q$ is true

We showed that

If m is an even integer then m^2 is an even integer

We showed that

If m is an even integer then m^2 is an even integer

Another way of saying this is that

For all even integers m, m^2 is also an even integer.

We showed that

If m is an even integer then m^2 is an even integer

Another way of saying this is that

For all even integers m, m^2 is also an even integer.

Principle 3.5 (Universal Generalization)
If we can prove a statement $p(x)$ about x by assuming only that x is a member of our universe, then we can conclude that $p(x)$ is true for every member of our universe.

3.3 Inference

- What is a Proof?
- Direct Inference (Modus Ponens)
- Rules of Inference for Direct Proofs
- Contrapositive Rule of Inference
- Proof by Contradiction

Rules of Inference for Direct Proofs

Rules of Inference for Direct Proofs

A **direct proof** consists of a sequence of statements, each of which is either a (i) hypothesis, a (ii) generally accepted fact, or (iii) the result of one of the following rules of inference for compound statements.

Rules of Inference for Direct Proofs

A **direct proof** consists of a sequence of statements, each of which is either a (i) hypothesis, a (ii) generally accepted fact, or (iii) the result of one of the following rules of inference for compound statements.

1. From an example x that does not satisfy $p(x)$,
   we may conclude $\neg p(x)$.

Rules of Inference for Direct Proofs

A **direct proof** consists of a sequence of statements, each of which is either a (i) hypothesis, a (ii) generally accepted fact, or (iii) the result of one of the following rules of inference for compound statements.

1. From an example x that does not satisfy $p(x)$,
   we may conclude $\neg p(x)$.

2. From $p(x)$ and $q(x)$,
   we may conclude $p(x) \wedge q(x)$.

Rules of Inference for Direct Proofs

A **direct proof** consists of a sequence of statements, each of which is either a (i) hypothesis, a (ii) generally accepted fact, or (iii) the result of one of the following rules of inference for compound statements.

1. From an example x that does not satisfy $p(x)$,
   we may conclude $\neg p(x)$.

2. From $p(x)$ and $q(x)$,
   we may conclude $p(x) \wedge q(x)$.

3. From either $p(x)$ or $q(x)$,
   we may conclude $p(x) \vee q(x)$.

Rules of Inference for Direct Proofs

A **direct proof** consists of a sequence of statements, each of which is either a (i) hypothesis, a (ii) generally accepted fact, or (iii) the result of one of the following rules of inference for compound statements.

1. From an example x that does not satisfy $p(x)$,
   we may conclude $\neg p(x)$.

2. From $p(x)$ and $q(x)$,
   we may conclude $p(x) \wedge q(x)$.

3. From either $p(x)$ or $q(x)$,
   we may conclude $p(x) \vee q(x)$.

4. From either $q(x)$ or $\neg p(x)$
   we may conclude $p(x) \Rightarrow q(x)$.

5. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow p(x)$,
we may conclude $p(x) \Leftrightarrow q(x)$.

5. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow p(x)$,
   we may conclude $p(x) \Leftrightarrow q(x)$.

6. From $p(x)$ and $p(x) \Rightarrow q(x)$,
   we may conclude $q(x)$.

5. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow p(x)$,
   we may conclude $p(x) \Leftrightarrow q(x)$.

6. From $p(x)$ and $p(x) \Rightarrow q(x)$,
   we may conclude $q(x)$.

7. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow r(x)$,
   we may conclude $p(x) \Rightarrow r(x)$.

5. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow p(x)$,
   we may conclude $p(x) \Leftrightarrow q(x)$.
6. From $p(x)$ and $p(x) \Rightarrow q(x)$,
   we may conclude $q(x)$.
7. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow r(x)$,
   we may conclude $p(x) \Rightarrow r(x)$.
8. If we can derive $q(x)$ from hypothesis that x satisfies $p(x)$,
   we may conclude $p(x) \Rightarrow q(x)$.

5. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow p(x)$,
   we may conclude $p(x) \Leftrightarrow q(x)$.

6. From $p(x)$ and $p(x) \Rightarrow q(x)$,
   we may conclude $q(x)$.

7. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow r(x)$,
   we may conclude $p(x) \Rightarrow r(x)$.

8. If we can derive $q(x)$ from hypothesis that x satisfies $p(x)$,
   we may conclude $p(x) \Rightarrow q(x)$.

9. If we can derive $p(x)$ from the hypothesis that
   x is a (generic) member of our universe U,
   we may conclude $\forall x \in U\ (p(x))$.

5. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow p(x)$,
   we may conclude $p(x) \Leftrightarrow q(x)$.

6. From $p(x)$ and $p(x) \Rightarrow q(x)$,
   we may conclude $q(x)$.

7. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow r(x)$,
   we may conclude $p(x) \Rightarrow r(x)$.

8. If we can derive $q(x)$ from hypothesis that x satisfies $p(x)$,
   we may conclude $p(x) \Rightarrow q(x)$.

9. If we can derive $p(x)$ from the hypothesis that
   x is a (generic) member of our universe U,
   we may conclude $\forall x \in U\, (p(x))$.

10. From an example of an $x \in U$ satisfying $p(x)$,
    we may conclude $\exists x \in U\, (p(x))$.

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer.

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer.

Setup for rule 9

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer.

Setup for rule 9

Suppose that m is even.

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. Setup for rule 9

Suppose that m is even. Implicit hypothesis

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. Setup for rule 9

Suppose that m is even. Implicit hypothesis

If m is even, then $\exists k$ with $m = 2k$.

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. Setup for rule 9

Suppose that m is even. Implicit hypothesis

If m is even, then $\exists k$ with $m = 2k$. Definition

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. Setup for rule 9

Suppose that m is even. Implicit hypothesis

If m is even, then $\exists k$ with $m = 2k$. Definition

Then $\exists k$ such that $m = 2k$.

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer.	Setup for rule 9
Suppose that m is even.	Implicit hypothesis
If m is even, then $\exists k$ with $m = 2k$.	Definition
Then $\exists k$ such that $m = 2k$.	Rule 6 (m.p.)

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer.	Setup for rule 9
Suppose that m is even.	Implicit hypothesis
If m is even, then $\exists k$ with $m = 2k$.	Definition
Then $\exists k$ such that $m = 2k$.	Rule 6 (m.p.)
Then $\exists k$ such that $m^2 = 4k^2$.	

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. — Setup for rule 9

Suppose that m is even. — Implicit hypothesis

If m is even, then $\exists k$ with $m = 2k$. — Definition

Then $\exists k$ such that $m = 2k$. — Rule 6 (m.p.)

Then $\exists k$ such that $m^2 = 4k^2$. — Algebra

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. Setup for rule 9

Suppose that m is even. Implicit hypothesis

If m is even, then $\exists k$ with $m = 2k$. Definition

Then $\exists k$ such that $m = 2k$. Rule 6 (m.p.)

Then $\exists k$ such that $m^2 = 4k^2$. Algebra

Then, there is an integer $h = 2k^2$ s.t. $m^2 = 2h$.

Algebra

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. Setup for rule 9

Suppose that m is even. Implicit hypothesis

If m is even, then $\exists k$ with $m = 2k$. Definition

Then $\exists k$ such that $m = 2k$. Rule 6 (m.p.)

Then $\exists k$ such that $m^2 = 4k^2$. Algebra

Then, there is an integer $h = 2k^2$ s.t. $m^2 = 2h$.

Algebra

Then, if m is even, then m^2 is even.

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. Setup for rule 9

Suppose that m is even. Implicit hypothesis

If m is even, then $\exists k$ with $m = 2k$. Definition

Then $\exists k$ such that $m = 2k$. Rule 6 (m.p.)

Then $\exists k$ such that $m^2 = 4k^2$. Algebra

Then, there is an integer $h = 2k^2$ s.t. $m^2 = 2h$.

Algebra

Then, if m is even, then m^2 is even. Rule 8

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. Setup for rule 9

Suppose that m is even. Implicit hypothesis

If m is even, then $\exists k$ with $m = 2k$. Definition

Then $\exists k$ such that $m = 2k$. Rule 6 (m.p.)

Then $\exists k$ such that $m^2 = 4k^2$. Algebra

Then, there is an integer $h = 2k^2$ s.t. $m^2 = 2h$.

Algebra

Then, if m is even, then m^2 is even. Rule 8

Then, $\forall m \in Z$, if m is even, then m^2 is even.

Prove that $\forall m \in Z$, if m is even, then m^2 is even.

Let m be an integer. Setup for rule 9

Suppose that m is even. Implicit hypothesis

If m is even, then $\exists k$ with $m = 2k$. Definition

Then $\exists k$ such that $m = 2k$. Rule 6 (m.p.)

Then $\exists k$ such that $m^2 = 4k^2$. Algebra

Then, there is an integer $h = 2k^2$ s.t. $m^2 = 2h$.

Algebra

Then, if m is even, then m^2 is even. Rule 8

Then, $\forall m \in Z$, if m is even, then m^2 is even. Rule 9

3.3 Inference

- What is a Proof?
- Direct Inference (Modus Ponens)
- Rules of Inference for Direct Proofs
- Contrapositive Rule of Inference
- Proof by Contradiction

Contrapositive Rule of Inference

Contrapositive Rule of Inference

$\neg q$ implies $\neg p$ is the contrapositive of p implies q

Contrapositive Rule of Inference

$\neg q$ implies $\neg p$ is the contrapositive of p implies q

p implies q is actually equivalent to $\neg q$ implies $\neg p$.

double truth table

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

Principle 3.6 (Proof by Contraposition)
The statements $p \Rightarrow q$ and $\neg q \Rightarrow \neg p$ are equivalent, and so a proof of one is a proof of the other.

Principle 3.6 (Proof by Contraposition)
The statements $p \Rightarrow q$ and $\neg q \Rightarrow \neg p$ are equivalent, and so a proof of one is a proof of the other.

We Adopt Principle 3.6 as a rule of inference, called the **contrapositive rule of inference**.

11. From $\neg q(x) \Rightarrow \neg p(x)$,
    we may conclude $p(x) \Rightarrow q(x)$.

Example:

If n is a positive integer with $n^2 > 100$, then $n > 10$.

Example:

If n is a positive integer with $\underset{p(x)}{n^2 > 100}$, then $\underset{q(x)}{n > 10}$.

Example:

If n is a positive integer with $\underbrace{n^2 > 100}_{p(x)}$, then $\underbrace{n > 10}_{q(x)}$.

Proof (by contraposition):

Example:

If n is a positive integer with $\underbrace{n^2 > 100}_{p(x)}$, then $\underbrace{n > 10}_{q(x)}$.

Proof (by contraposition):

Suppose n is not greater than 10.

Example:

If n is a positive integer with $n^2 > 100$, then $n > 10$.

$p(x)$ $q(x)$

Proof (by contraposition):

Suppose n is not greater than 10. $\neg q(x)$

Example:

If n is a positive integer with $n^2 > 100$, then $n > 10$.

$p(x)$ $q(x)$

Proof (by contraposition):

Suppose n is not greater than 10. $\neg q(x)$

Then, because $1 \leq n \leq 10$, we have $n \cdot n \leq n \cdot 10 \leq 10 \cdot 10 = 100$.

(Using: "If $x \leq y$ and $c \geq 0$, then $cx \leq cy$.")

Example:

If n is a positive integer with $n^2 > 100$, then $n > 10$.

$p(x)$ $q(x)$

Proof (by contraposition):

Suppose n is not greater than 10. $\neg q(x)$

Then, because $1 \leq n \leq 10$, we have $n \cdot n \leq n \cdot 10 \leq 10 \cdot 10 = 100$.

(Using: "If $x \leq y$ and $c \geq 0$, then $cx \leq cy$.")

Thus, n^2 is not greater than 100.

Example:

If n is a positive integer with $\underbrace{n^2 > 100}_{p(x)}$, then $\underbrace{n > 10}_{q(x)}$.

Proof (by contraposition):

Suppose n is not greater than 10. $\neg q(x)$

Then, because $1 \leq n \leq 10$, we have $n \cdot n \leq n \cdot 10 \leq 10 \cdot 10 = 100$.

(Using: "If $x \leq y$ and $c \geq 0$, then $cx \leq cy$.")

Thus, n^2 is not greater than 100. $\neg p(x)$

Example:

If n is a positive integer with $n^2 > 100$, then $n > 10$.

$p(x)$ $q(x)$

Proof (by contraposition):

Suppose n is not greater than 10. $\neg q(x)$

Then, because $1 \leq n \leq 10$, we have $n \cdot n \leq n \cdot 10 \leq 10 \cdot 10 = 100$.

(Using: "If $x \leq y$ and $c \geq 0$, then $cx \leq cy$.")

Thus, n^2 is not greater than 100. $\neg p(x)$

Thus, if $n \not> 10$ then $n^2 \not> 100$

Example:

If n is a positive integer with $\underset{p(x)}{n^2 > 100}$, then $\underset{q(x)}{n > 10}$.

Proof (by contraposition):

Suppose n is not greater than 10. $\neg q(x)$

Then, because $1 \leq n \leq 10$, we have $n \cdot n \leq n \cdot 10 \leq 10 \cdot 10 = 100$.

(Using: "If $x \leq y$ and $c \geq 0$, then $cx \leq cy$.")

Thus, n^2 is not greater than 100. $\neg p(x)$

Thus, if $n \not> 10$ then $n^2 \not> 100$ $\neg q(x) \Rightarrow \neg p(x)$

Example:

If n is a positive integer with $n^2 > 100$, then $n > 10$.

$p(x)$ $q(x)$

Proof (by contraposition):

Suppose n is not greater than 10. $\neg q(x)$

Then, because $1 \leq n \leq 10$, we have $n \cdot n \leq n \cdot 10 \leq 10 \cdot 10 = 100$.

(Using: "If $x \leq y$ and $c \geq 0$, then $cx \leq cy$.")

Thus, n^2 is not greater than 100. $\neg p(x)$

Thus, if $n \not> 10$ then $n^2 \not> 100$ $\neg q(x) \Rightarrow \neg p(x)$

By the principle of proof by contraposition,
if $n^2 > 100$, then $n > 10$.

Example:

If n is a positive integer with $n^2 > 100$, then $n > 10$.

$p(x)$ $q(x)$

Proof (by contraposition):

Suppose n is not greater than 10. $\neg q(x)$

Then, because $1 \leq n \leq 10$, we have $n \cdot n \leq n \cdot 10 \leq 10 \cdot 10 = 100$.

(Using: "If $x \leq y$ and $c \geq 0$, then $cx \leq cy$.")

Thus, n^2 is not greater than 100. $\neg p(x)$

Thus, if $n \not> 10$ then $n^2 \not> 100$ $\neg q(x) \Rightarrow \neg p(x)$

By the principle of proof by contraposition,

if $n^2 > 100$, then $n > 10$. $p(x) \Rightarrow q(x)$

Is p implies q equivalent to q implies p?

Is p implies q equivalent to q implies p? No!

double truth table

p	q	$p \Rightarrow q$	$q \Rightarrow p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Is p implies q equivalent to q implies p? No!

double truth table

p	q	$p \Rightarrow q$	$q \Rightarrow p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Example: $p(x) \sim (x$ is a cat$)$ and $q(x) \sim (x$ has 4 legs$)$

Is p implies q equivalent to q implies p? No!

double truth table

p	q	$p \Rightarrow q$	$q \Rightarrow p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Example: $p(x) \sim$ (x is a cat) and $q(x) \sim$ (x has 4 legs)

$p(x) \Rightarrow q(x)$: If x is a cat then x has four legs

$q(x) \Rightarrow p(x)$: If x has 4 legs then x is a cat

Is p implies q equivalent to q implies p? No!

double truth table

p	q	$p \Rightarrow q$	$q \Rightarrow p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Example: $p(x) \sim$ (x is a cat) and $q(x) \sim$ (x has 4 legs)

$p(x) \Rightarrow q(x)$: If x is a cat then x has four legs

$q(x) \Rightarrow p(x)$: If x has 4 legs then x is a cat

$q \Rightarrow p$ is called the **converse** of $p \Rightarrow q$.

3.3 Inference

- What is a Proof?
- Direct Inference (Modus Ponens)
- Rules of Inference for Direct Proofs
- Contrapositive Rule of Inference
- Proof by Contradiction

Proof by Contradiction

Proof by Contradiction

- Start by assuming the statement is False.

Proof by Contradiction

- Start by assuming the statement is False.
- From that assumption derive a contradiction
  (to the assumption itself).

Proof by Contradiction

- Start by assuming the statement is False.
- From that assumption derive a contradiction
  (to the assumption itself).
- Because all reasoning, except for the assumption that the statement is False, used accepted rules of inference, the only source of contradiction is the assumption itself.

Proof by Contradiction

- Start by assuming the statement is False.
- From that assumption derive a contradiction
  (to the assumption itself).
- Because all reasoning, except for the assumption that the statement is False, used accepted rules of inference, the only source of contradiction is the assumption itself.
- Thus, by the principle of the excluded middle,
  the assumption has to be incorrect.

Proof by Contradiction

- Start by assuming the statement is False.
- From that assumption derive a contradiction
  (to the assumption itself).
- Because all reasoning, except for the assumption that the statement is False, used accepted rules of inference, the only source of contradiction is the assumption itself.
- Thus, by the principle of the excluded middle,
  the assumption has to be incorrect.
- Adopt the principle of proof by contradiction (also called the principle of reduction to absurdity) as last rule of inference

Proof by Contradiction

- Start by assuming the statement is False.
- From that assumption derive a contradiction
  (to the assumption itself).
- Because all reasoning, except for the assumption that the statement is False, used accepted rules of inference, the only source of contradiction is the assumption itself.
- Thus, by the principle of the excluded middle,
  the assumption has to be incorrect.
- Adopt the principle of proof by contradiction (also called the principle of reduction to absurdity) as last rule of inference

12. If by assuming $p(x)$ and $\neg q(x)$, we can derive both $r(x)$ and $\neg r(x)$ for some statement $r(x)$, we may conclude $p(x) \Rightarrow q(x)$.

Some variations of *proof by contradiction*

Some variations of *proof by contradiction*

These variations are all examples of what we call indirect proofs.

Some variations of *proof by contradiction*

These variations are all examples of what we call indirect proofs.

We will now see 3 different proofs by contradiction that $p \Rightarrow q$ where p is the statement $x^2 + x - 2 = 0$, and q is the statement $x \neq 0$.

Some variations of *proof by contradiction*

These variations are all examples of what we call indirect proofs.

We will now see 3 different proofs by contradiction that $p \Rightarrow q$ where p is the statement $x^2 + x - 2 = 0$, and q is the statement $x \neq 0$.

Each of the three proofs by contradiction work by getting sightly different contradictions.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

1. We will assume p is True and q is False;
   from this, we derive a contradiction by proving that p is False.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

1. We will assume p is True and q is False; from this, we derive a contradiction by proving that p is False.

Proof:

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

1. We will assume p is True and q is False;
   from this, we derive a contradiction by proving that p is False.

Proof:

Assume that (i) $x^2 + x - 2 = 0$ and (ii) $x = 0$

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

1. We will assume p is True and q is False;
   from this, we derive a contradiction by proving that p is False.

Proof:

Assume that (i) $x^2 + x - 2 = 0$ and (ii) $x = 0$

Substituting 0 for x in the polynomial gives
$$x^2 + x - 2 = 0 + 0 - 2 = -2.$$

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

1. We will assume p is True and q is False;
   from this, we derive a contradiction by proving that p is False.

Proof:

Assume that (i) $x^2 + x - 2 = 0$ and (ii) $x = 0$

Substituting 0 for x in the polynomial gives

$$x^2 + x - 2 = 0 + 0 - 2 = -2.$$

This contradicts assumption $x^2 + x - 2 = 0$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

1. We will assume p is True and q is False;
   from this, we derive a contradiction by proving that p is False.

Proof:

Assume that (i) $x^2 + x - 2 = 0$ and (ii) $x = 0$

Substituting 0 for x in the polynomial gives
$x^2 + x - 2 = 0 + 0 - 2 = -2$.

This contradicts assumption $x^2 + x - 2 = 0$.

Thus, by the principle of proof by contradiction,
if $x^2 + x - 2 = 0$, then $x \neq 0$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

2. We will assume p is True and q is False;
   from this, we derive a contradiction of a known fact

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

2. We will assume p is True and q is False;
   from this, we derive a contradiction of a known fact

Proof:

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

2. We will assume p is True and q is False;
   from this, we derive a contradiction of a known fact

Proof:

Assume that (i) $x^2 + x - 2 = 0$ and (ii) $x = 0$

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

2. We will assume p is True and q is False;
   from this, we derive a contradiction of a known fact

Proof:

Assume that (i) $x^2 + x - 2 = 0$ and (ii) $x = 0$

Substituting 0 for x in the polynomial gives

$$x^2 + x - 2 = 0 + 0 - 2 = -2.$$

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

2. We will assume p is True and q is False;
   from this, we derive a contradiction of a known fact

Proof:

Assume that (i) $x^2 + x - 2 = 0$ and (ii) $x = 0$

Substituting 0 for x in the polynomial gives
$$x^2 + x - 2 = 0 + 0 - 2 = -2.$$

Thus, $0 = -2$, which is a contradiction.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

2. We will assume p is True and q is False;
   from this, we derive a contradiction of a known fact

Proof:

Assume that (i) $x^2 + x - 2 = 0$ and (ii) $x = 0$

Substituting 0 for x in the polynomial gives
$x^2 + x - 2 = 0 + 0 - 2 = -2$.

Thus, $0 = -2$, which is a contradiction.

Thus, by the principle of proof by contradiction,
if $x^2 + x - 2 = 0$, then $x \neq 0$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

3. We will again assume p is True and q is False;

Sometimes contradiction statement r is simply a statement that arises naturally as we try to construct our proof.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

3. We will again assume p is True and q is False;

Sometimes contradiction statement r is simply a statement that arises naturally as we try to construct our proof.

Proof:

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

3. We will again assume p is True and q is False;
Sometimes contradiction statement r is simply a statement that arises naturally as we try to construct our proof.

Proof:

Suppose that $x^2 + x - 2 = 0$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

3. We will again assume p is True and q is False;
Sometimes contradiction statement r is simply a statement that arises naturally as we try to construct our proof.

Proof:

Suppose that $x^2 + x - 2 = 0$. Then $x^2 + x = 2$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

3. We will again assume p is True and q is False;
Sometimes contradiction statement r is simply a statement that arises naturally as we try to construct our proof.

Proof:

Suppose that $x^2 + x - 2 = 0$. Then $x^2 + x = 2$.

Assume that $x = 0$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

3. We will again assume p is True and q is False;
Sometimes contradiction statement r is simply a statement that arises naturally as we try to construct our proof.

Proof:

Suppose that $x^2 + x - 2 = 0$. Then $x^2 + x = 2$.

Assume that $x = 0$.

Substituting 0 for x in $x^2 + x$ gives

$$x^2 + x = 0 + 0 = 0.$$

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

3. We will again assume p is True and q is False;
Sometimes contradiction statement r is simply a statement that arises naturally as we try to construct our proof.

Proof:

Suppose that $x^2 + x - 2 = 0$. Then $x^2 + x = 2$.

Assume that $x = 0$.

Substituting 0 for x in $x^2 + x$ gives

$$x^2 + x = 0 + 0 = 0.$$

This contradicts our observation that $x^2 + x = 2$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

3. We will again assume p is True and q is False;
Sometimes contradiction statement r is simply a statement that arises naturally as we try to construct our proof.

Proof:

Suppose that $x^2 + x - 2 = 0$. Then $x^2 + x = 2$.

Assume that $x = 0$.

Substituting 0 for x in $x^2 + x$ gives

$$x^2 + x = 0 + 0 = 0.$$

This contradicts our observation that $x^2 + x = 2$.

Thus, by the principle of proof by contradiction,
if $x^2 + x - 2 = 0$, then $x \neq 0$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

4. Finally, if you think that proof by contradiction seems similar to proof by contraposition, you are right.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

4. Finally, if you think that proof by contradiction seems similar to proof by contraposition, you are right.

Proof:

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

4. Finally, if you think that proof by contradiction seems similar to proof by contraposition, you are right.

Proof:

Assume that $x = 0$. $\neg q(x)$

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

4. Finally, if you think that proof by contradiction seems similar to proof by contraposition, you are right.

Proof:

Assume that $x = 0$. $\neg q(x)$

Then $x^2 + x - 2 = 0 + 0 - 2 = -2$.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

4. Finally, if you think that proof by contradiction seems similar to proof by contraposition, you are right.

Proof:

Assume that $x = 0$. $\neg q(x)$

Then $x^2 + x - 2 = 0 + 0 - 2 = -2$.

Then $x^2 + x - 2 \neq 0$. $\neg p(x)$

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

4. Finally, if you think that proof by contradiction seems similar to proof by contraposition, you are right.

Proof:

Assume that $x = 0$. $\neg q(x)$

Then $x^2 + x - 2 = 0 + 0 - 2 = -2$.

Then $x^2 + x - 2 \neq 0$. $\neg p(x)$

Thus, by the principle of proof by contraposition,
if $x^2 + x - 2 = 0$, then $x \neq 0$. $p(x) \Rightarrow q(x)$

Any proof that uses one of the indirect methods of inference, either contradiction or contraposition, is called an **indirect proof**.

Any proof that uses one of the indirect methods of inference, either contradiction or contraposition, is called an **indirect proof**.

Example:

Without extracting square roots, prove that if n is a positive integer such that $n^2 < 9$, then $n < 3$.

Any proof that uses one of the indirect methods of inference, either contradiction or contraposition, is called an **indirect proof**.

Example:

Without extracting square roots, prove that if n is a positive integer such that $n^2 < 9$, then $n < 3$.

Assume, for purposes of contradiction, that $n \geq 3$.

Any proof that uses one of the indirect methods of inference, either contradiction or contraposition, is called an **indirect proof**.

Example:
Without extracting square roots, prove that if n is a positive integer such that $n^2 < 9$, then $n < 3$.

Assume, for purposes of contradiction, that $n \geq 3$.

Squaring both sides, we obtain $n^2 \geq 9$.

Any proof that uses one of the indirect methods of inference, either contradiction or contraposition, is called an **indirect proof**.

Example:

Without extracting square roots, prove that if n is a positive integer such that $n^2 < 9$, then $n < 3$.

Assume, for purposes of contradiction, that $n \geq 3$.

Squaring both sides, we obtain $n^2 \geq 9$.

This contradicts our hypothesis that $n^2 < 9$.

Any proof that uses one of the indirect methods of inference, either contradiction or contraposition, is called an **indirect proof**.

Example:

Without extracting square roots, prove that if n is a positive integer such that $n^2 < 9$, then $n < 3$.

Assume, for purposes of contradiction, that $n \geq 3$.

Squaring both sides, we obtain $n^2 \geq 9$.

This contradicts our hypothesis that $n^2 < 9$.

Therefore, by principle of proof by contradiction, $n < 3$.

Prove that $\sqrt{5}$ is not rational.

Prove that $\sqrt{5}$ is not rational.

Assume, for purpose of contradiction, that $\sqrt{5}$ is rational.

Prove that $\sqrt{5}$ is not rational.

Assume, for purpose of contradiction, that $\sqrt{5}$ is rational.

This means that we can write $\sqrt{5} = m/n$,
where m and n are integers.

Prove that $\sqrt{5}$ is not rational.

Assume, for purpose of contradiction, that $\sqrt{5}$ is rational.

This means that we can write $\sqrt{5} = m/n$,
where m and n are integers.

Squaring both sides of $\sqrt{5} = m/n$, we obtain $\frac{m^2}{n^2} = 5$, or $m^2 = 5n^2$.

Prove that $\sqrt{5}$ is not rational.

Assume, for purpose of contradiction, that $\sqrt{5}$ is rational.

This means that we can write $\sqrt{5} = m/n$,
where m and n are integers.

Squaring both sides of $\sqrt{5} = m/n$, we obtain $\frac{m^2}{n^2} = 5$, or $m^2 = 5n^2$.

m^2 and n^2 must each have an even number of prime factors
(counting each prime factor as many times as it occurs).

Prove that $\sqrt{5}$ is not rational.

Assume, for purpose of contradiction, that $\sqrt{5}$ is rational.

This means that we can write $\sqrt{5} = m/n$,
where m and n are integers.

Squaring both sides of $\sqrt{5} = m/n$, we obtain $\frac{m^2}{n^2} = 5$, or $m^2 = 5n^2$.

m^2 and n^2 must each have an even number of prime factors (counting each prime factor as many times as it occurs).

But $5n^2$ has an odd number of prime factors.

Prove that $\sqrt{5}$ is not rational.

Assume, for purpose of contradiction, that $\sqrt{5}$ is rational.

This means that we can write $\sqrt{5} = m/n$,
where m and n are integers.

Squaring both sides of $\sqrt{5} = m/n$, we obtain $\frac{m^2}{n^2} = 5$, or $m^2 = 5n^2$.

m^2 and n^2 must each have an even number of prime factors (counting each prime factor as many times as it occurs).

But $5n^2$ has an odd number of prime factors.

Thus, a product of an even number of prime factors is equal to a product of an odd number of prime factors

Prove that $\sqrt{5}$ is not rational.

Assume, for purpose of contradiction, that $\sqrt{5}$ is rational.

This means that we can write $\sqrt{5} = m/n$,
where m and n are integers.

Squaring both sides of $\sqrt{5} = m/n$, we obtain $\frac{m^2}{n^2} = 5$, or $m^2 = 5n^2$.

m^2 and n^2 must each have an even number of prime factors (counting each prime factor as many times as it occurs).

But $5n^2$ has an odd number of prime factors.

Thus, a product of an even number of prime factors is equal to a product of an odd number of prime factors

A contradiction, because each positive integer may be expressed uniquely as a product of (positive) prime numbers.

Prove that $\sqrt{5}$ is not rational.

Assume, for purpose of contradiction, that $\sqrt{5}$ is rational.

This means that we can write $\sqrt{5} = m/n$,
where m and n are integers.

Squaring both sides of $\sqrt{5} = m/n$, we obtain $\frac{m^2}{n^2} = 5$, or $m^2 = 5n^2$.

m^2 and n^2 must each have an even number of prime factors (counting each prime factor as many times as it occurs).

But $5n^2$ has an odd number of prime factors.

Thus, a product of an even number of prime factors is equal to a product of an odd number of prime factors

A contradiction, because each positive integer may be expressed uniquely as a product of (positive) prime numbers.

Thus, by the principle of proof by contradiction, $\sqrt{5}$ is not rational.