CSE 191

Introduction to Discrete Structures

Dr. Eric Mikida
epmikida@buffalo.edu
208 Capen Hall

Logical Reasoning and Proof Methods

Outline

- **Logical Reasoning**
  - **Definition**
  - Invalid Argument
  - Logical Reasoning Rules
  - Logical Reasoning Example
- Introduction to Mathematical Proofs

Logical Reasoning: What is it?

Suppose the following are TRUE statements:

1. You will buy your friend lunch if they drive you to work
2. They drove you to work

What can you conclude?

Logical Reasoning: What is it?

Suppose the following are TRUE statements:

1. You will buy your friend lunch if they drive you to work
2. They drove you to work

What can you conclude?

You will buy your friend lunch.

Logical Reasoning: What is it?

Suppose the following are TRUE statements:

1. You will buy your friend lunch if they drive you to work
2. They drove you to work

What can you conclude?

You will buy your friend lunch.

Note: This differs from logical equivalence

- Statements derived are not always equivalent
- Can derive new knowledge from multiple facts

Logical Reasoning: What is it?

Suppose the following are TRUE statements:

1. You will buy your friend lunch if they drive you to work
2. They drove you to work

What can you conclude?

You will buy your friend lunch.

Note: This differs from logical equivalence

- Statements derived are not always equivalent
- Can derive new knowledge from multiple facts

Also known as deductive reasoning

Logical Reasoning: Arguments

Arguments are:

- a list of propositions, called **hypotheses** (also called **premises**)
- a final proposition, called the **conclusion**

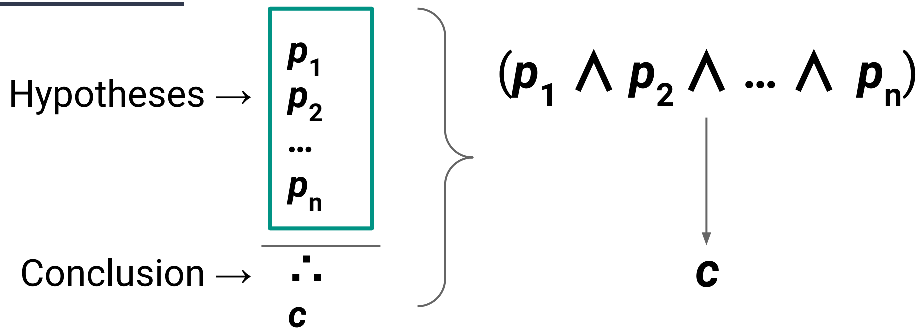
Hypotheses → p_1, p_2, …, p_n

Conclusion → $\therefore$ c

Logical Reasoning: Arguments

Arguments are:

- a list of propositions, called **hypotheses** (also called **premises**)
- a final proposition, called the **conclusion**



An argument is **valid** if $(p_1 \land p_2 \land \ldots \land p_n) \rightarrow c$ is a tautology

- Otherwise, it is **invalid**
- **Fallacies** are incorrect reasonings which lead to invalid arguments

Logical Reasoning: Example

You will buy your friend lunch if they drive you to work

They drove you to work

∴ You will buy your friend lunch

Logical Reasoning: Example

You will buy your friend lunch if they drive you to work

They drove you to work

∴ You will buy your friend lunch

p: You will buy your friend lunch

q: They drove you to work

Logical Reasoning: Example

You will buy your friend lunch if they drive you to work

They drove you to work

∴ You will buy your friend lunch

$$\begin{array}{c} q \rightarrow p \\ q \\ \hline \therefore p \end{array}$$

Form of the argument

p: You will buy your friend lunch

***q*:** They drove you to work

Logical Reasoning: Example

You will buy your friend lunch if they drive you to work

They drove you to work

∴ You will buy your friend lunch

$$\begin{array}{c} \boldsymbol{q \rightarrow p} \\ \boldsymbol{q} \\ \hline \therefore \boldsymbol{p} \end{array}$$

Form of the argument

p: You will buy your friend lunch

q: They drove you to work

$((\boldsymbol{q} \rightarrow \boldsymbol{p}) \land \boldsymbol{q}) \rightarrow \boldsymbol{p}$ is a tautology, therefore the argument is valid

Logical Reasoning: Simplest Example

Prove that the following is a valid argument:

$$\begin{array}{c} p \\ \hline \therefore p \end{array}$$

Logical Reasoning: Simplest Example

Prove that the following is a valid argument:

$$\frac{\boldsymbol{p}}{\therefore \boldsymbol{p}}$$

Proving this argument is the same as proving $\boldsymbol{p} \rightarrow \boldsymbol{p}$ is a tautology

Logical Reasoning: Simplest Example

Prove that the following is a valid argument:

$$\frac{\boldsymbol{p}}{\therefore \boldsymbol{p}}$$

Proving this argument is the same as proving $\boldsymbol{p} \rightarrow \boldsymbol{p}$ is a tautology

$\boldsymbol{p}$	$\boldsymbol{p} \rightarrow \boldsymbol{p}$
F	T
T	T

Therefore, we have shown it's a valid argument

Logical Reasoning: Another Simple Example

Consider the contrapositive as a logical argument

$$\frac{p \to q}{\therefore \neg q \to \neg p}$$

$$\frac{\neg q \to \neg p}{\therefore p \to q}$$

Proof of Validity:

1. $p \to q$ Hypothesis
2. $\neg p \lor q$ Conditional law
3. $q \lor \neg p$ Commutative law
4. $\neg\neg q \lor \neg p$ Double negation law
5. $\neg q \to \neg p$ Conditional law

Proof of Validity:

1. $\neg q \to \neg p$ Hypothesis
2. $\neg\neg q \lor \neg p$ Conditional law
3. $q \lor \neg p$ Double negation law
4. $\neg p \lor q$ Commutative law
5. $p \to q$ Conditional law

Logical Reasoning: Another Simple Example

Consider the contrapositive as a logical argument

$$\frac{p \rightarrow q}{\therefore \neg q \rightarrow \neg p}$$

$$\frac{\neg q \rightarrow \neg p}{\therefore p \rightarrow q}$$

Proof of Validity:

1.	$p \rightarrow q$	Hypothesis
2.	$\neg p \lor q$	Conditional law
3.	$q \lor \neg p$	Commutative law
4.	$\neg\neg q \lor \neg p$	Double negation law
5.	$\neg q \rightarrow \neg p$	Conditional law

Proof of Validity:

1.	$\neg q \rightarrow \neg p$	Hypothesis
2.	$\neg\neg q \lor \neg p$	Conditional law
3.	$q \lor \neg p$	Double negation law
4.	$\neg p \lor q$	Commutative law
5.	$p \rightarrow q$	Conditional law

Note: Here we've shown that the hypothesis is equivalent to the conclusion…this is actually overkill

Logical Reasoning: Proof Definition

A **logical proof** of an argument is a sequence of steps, each of which consists of a proposition and a justification

Logical Reasoning: Proof Definition

A **logical proof** of an argument is a sequence of steps, each of which consists of a proposition and a justification

Each line should contain one of the following:

- a hypothesis (assumption)
- a proposition that is equivalent to a previous statement
- a proposition that is derived by applying an argument to previous statements

Logical Reasoning: Proof Definition

A **<u>logical proof</u>** of an argument is a sequence of steps, each of which consists of a proposition and a justification

Each line should contain one of the following:

- a hypothesis (assumption)
- a proposition that is equivalent to a previous statement
- a proposition that is derived by applying an argument to previous statements

Jusificiations should state one of the following:

- hypothesis
- the equivalence law used (and the line it was applied to)
- the argument used (and the line(s) it was applied to)

Logical Reasoning: Proof Definition

A **logical proof** of an argument is a sequence of steps, each of which consists of a proposition and a justification

Each line should contain one of the following:

- a hypothesis (assumption)
- a proposition that is equivalent to a previous statement
- a proposition that is derived by applying an argument to previous statements

Jusificiations should state one of the following:

- hypothesis
- the equivalence law used (and the line it was applied to)
- the argument used (and the line(s) it was applied to)

The last line should be the conclusion

Outline

- **Logical Reasoning**
  - Definition
  - **Invalid Argument**
  - Logical Reasoning Rules
  - Logical Reasoning Example
- Introduction to Mathematical Proofs

Logical Reasoning: Invalid Argument

How can we prove an argument is invalid?

Logical Reasoning: Invalid Argument

Remember: An argument is valid if $(\boldsymbol{p}_1 \land \boldsymbol{p}_2 \land \ldots \land \boldsymbol{p}_n) \rightarrow \boldsymbol{c}$ is a tautology

Therefore to show it is invalid, we need a **counterexample**. A counterexample is a situation where the hypotheses are all TRUE, and the conclusion is FALSE.

Logical Reasoning: Invalid Argument

Remember: An argument is valid if $(p_1 \land p_2 \land \ldots \land p_n) \rightarrow c$ is a tautology

Therefore to show it is invalid, we need a **counterexample**. A counterexample is a situation where the hypotheses are all TRUE, and the conclusion is FALSE.

Example consider the converse as an argument.

$$\frac{p \rightarrow q}{\therefore q \rightarrow p}$$

Logical Reasoning: Invalid Argument

Remember: An argument is valid if $(p_1 \land p_2 \land \ldots \land p_n) \to c$ is a tautology

Therefore to show it is invalid, we need a **counterexample**. A counterexample is a situation where the hypotheses are all TRUE, and the conclusion is FALSE.

Example consider the converse as an argument.

$$\frac{p \to q}{\therefore q \to p}$$

Suppose p: FALSE and q: TRUE.
Then $p \to q$ is TRUE, but $q \to p$ is FALSE.
Therefore the argument is invalid.

Outline

- **Logical Reasoning**
  - Definition
  - Invalid Argument
  - **Logical Reasoning Rules**
  - Logical Reasoning Example
- Introduction to Mathematical Proofs

Logical Reasoning: Rules of Inference

Rule of Inference	Name
p $p \rightarrow q$ $\therefore q$	Modus Ponens
$\neg q$ $p \rightarrow q$ $\therefore \neg p$	Modus Tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	Hypothetical Syllogism

Logical Reasoning: Rules of Inference

Rule of Inference	Name
$p \lor q$ $\neg p$ $\therefore q$	Disjunctive Syllogism
p $\therefore p \lor q$	Addition
$p \land q$ $\therefore p$	Simplification

Logical Reasoning: Rules of Inference

Rule of Inference	Name
p q $\therefore p \land q$	Conjunction
$p \lor q$ $\neg p \lor r$ $\therefore q \lor r$	Resolution

Outline

- **Logical Reasoning**
  - Definition
  - Invalid Argument
  - Logical Reasoning Rules
  - **Logical Reasoning Example**
- Introduction to Mathematical Proofs

Logical Reasoning Proofs

Using **modus ponens:**

$$\begin{array}{c} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

prove **modus tollens:**

$$\begin{array}{c} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$$

Logical Reasoning Proofs

Using **modus ponens:**

$$\frac{\begin{array}{c} p \\ p \rightarrow q \end{array}}{\therefore q}$$

prove **modus tollens:**

$$\frac{\begin{array}{c} \neg q \\ p \rightarrow q \end{array}}{\therefore \neg p}$$

Proof:

1. $\neg q$ Hypothesis
2. $p \rightarrow q$ Hypothesis
3. $\neg q \rightarrow \neg p$ Contrapositive, 2
4. $\neg p$ Modus ponens, 3,1

Logical Reasoning Proofs

Using **modus ponens:**

$$\begin{array}{c} p \\ p \rightarrow q \\ \hline \therefore q \rightarrow p \end{array}$$

prove **modus tollens:**

$$\begin{array}{c} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$$

Numbered steps

Proof:

1.	$\neg q$	Hypothesis
2.	$p \rightarrow q$	Hypothesis
3.	$\neg q \rightarrow \neg p$	Contrapositive, 2
4.	$\neg p$	Modus ponens, 3,1

Justification for each step, referencing relevant lines

Last line is the conclusion

Logical Reasoning Proofs

Prove the validity of the following argument:

If you send me an email, then I will finish writing the program

If you do not send me and email, then I will go to sleep early

If I go to sleep early, then I will wake up refreshed

∴ If I do not finish writing the program, then I will wake up refreshed

Logical Reasoning Proofs

Prove the validity of the following argument:

If you send me an email, then I will finish writing the program

If you do not send me and email, then I will go to sleep early

If I go to sleep early, then I will wake up refreshed

∴ If I do not finish writing the program, then I will wake up refreshed

***p*:** You send me an email
q: I will finish writing the program
r: I will go to sleep early
s: I will wake up feeling refreshed

Logical Reasoning Proofs

Prove the validity of the following argument:

If you send me an email, then I will finish writing the program

If you do not send me and email, then I will go to sleep early

If I go to sleep early, then I will wake up refreshed

∴ If I do not finish writing the program, then I will wake up refreshed

p: You send me an email
q: I will finish writing the program
r: I will go to sleep early
s: I will wake up feeling refreshed

$$p \rightarrow q$$
$$\neg p \rightarrow r$$
$$r \rightarrow s$$
$$\therefore \neg q \rightarrow s$$

Logical Reasoning Proofs

Proof

1. $p \rightarrow q$ Hypothesis
2. $\neg q \rightarrow \neg p$ Contrapositive, 1
3. $\neg p \rightarrow r$ Hypothesis
4. $\neg q \rightarrow r$ Hypothetical Syllogism, 2, 3
5. $r \rightarrow s$ Hypothesis
6. $\neg q \rightarrow s$ Hypothetical Syllogism, 4, 5

$$\begin{array}{c} p \rightarrow q \\ \neg p \rightarrow r \\ r \rightarrow s \\ \hline \therefore \neg q \rightarrow s \end{array}$$

Logical Reasoning Proofs

Proof that the following argument is valid:

$(\neg f \lor \neg r) \rightarrow (h \land t)$

$\neg t$

$\therefore r$

Logical Reasoning Proofs

Proof that the following argument is valid:

$(\neg f \lor \neg r) \to (h \land t)$
$\neg t$
$\therefore r$

Proof:

1. $(\neg f \lor \neg r) \to (h \land t)$ Hypothesis
2. $\neg(f \land r) \to (h \land t)$ De Morgan's Law, 1
3. $\neg(h \land t) \to (f \land r)$ Contrapositive, 2
4. $(\neg h \lor \neg t) \to (f \land r)$ De Morgan's Law, 3
5. $\neg t$ Hypothesis
6. $(\neg h \lor \neg t)$ Addition, 5
7. $(f \land r)$ Modus ponens, 4, 6
8. r Simplification, 7

Outline

- Logical Reasoning
- **Introduction to Mathematical Proofs**
    - **Terminology**
    - Proof by Exhaustion
    - Disproof by Counterexample
    - Direct Proofs
    - Proof by Contraposition
    - Proof by Contradiction

Mathematical Proofs

- A **mathematical proof** is usually "informal"
- More formal than everyday language, less formal than logical proofs
  - More than one rule may be used in a step
  - (**Some**) steps may be skipped
  - Axioms may be assumed
  - Rules for inference need not be explicitly stated
- Proofs must be a self-contained line of reasoning containing only:
  - facts (axioms)
  - Theorems, lemmas, corollaries (previously proven statements), or
  - statements derived from the above

You cannot use something as fact within a proof if you are not certain that it is

Some Terminology

- **Theorem**: statement that can be shown true
    - **Proposition**: less important theorem
    - **Lemma**: less important theorem used to prove other theorems
    - **Corollary**: theorem that trivially follows another theorem
- **Conjecture**: statement proposed to be true, but not yet proven
- **Axiom**: statement assumed to be true (does not need a proof)
- Most axioms, theorems, etc are universal over some domain
    - ie all perfect squares are non-negative
    - the domain should be clear from context, or explicitly stated

Hidden Universal Quantifier

<u>Example Theorem</u>: If $a > b$, then $a - b > 0$

[For all real numbers ***a*** and ***b***] if $a > b$, then $a - b > 0$

With predicates:

- $P(a, b)$: $a > b$
- $Q(a, b)$: $a - b > 0$
- **Theorem:** $\forall a,b, (P(a, b) \rightarrow Q(a, b))$

We can assume a general domain, $\mathbb{R}$ (real numbers), because nothing was stated otherwise

Outline

- Logical Reasoning
- **Introduction to Mathematical Proofs**
    - Terminology
    - **Proof by Exhaustion**
    - Disproof by Counterexample
    - Direct Proofs
    - Proof by Contraposition
    - Proof by Contradiction

Proof Method: Proof by Exhaustion

A **proof by exhaustion** for $p \rightarrow q$ starts by considering each element of the domain of discourse and showing the predicate is true

Only useful when dealing with a small domain

- Small is relative, but must be finite
- Example: {2,4,6} is a small and finite domain

This is a special type of *proof by cases*

Proof by Exhaustion Example

Prove that if ***n*** is in the domain {2,4,6}, then **3*n* ≤ 18**

Proof idea: Show the predicate is true for ***n* = 2**, ***n* = 6**, and ***n* = 6**

Proof:

***n* = 2: 3*n* = 3(2) = 6**. We know **6 ≤ 18**.

***n* = 4: 3*n* = 3(4) = 12**. We know **12 ≤ 18**.

***n* = 6: 3*n* = 3(6) = 18**. We know **18 ≤ 18**.

∴ for all possible values of ***n***, **3*n* ≤ 18**

Proof by Exhaustion Non-Example

Prove that if n has the form x^2 for some integer, x, then $n > 0$

Proof:

$n = 4$: Let **$x = 2$**, so $x^2 = 2^2 = 4.\ 4 > 0$

$n = 625$: Let **$x = 25$**, so $x^2 = 25^2 = 625.\ 625 > 0$

$n = 900$: Let **$x = -30$**, so $x^2 = -30^2 = 900.\ 900 > 0$

∴ If $n = x^2$ for some integer x, then $n > 0$

Proof by Exhaustion Non-Example

Prove that if ***n*** has the form x^2 for some integer, ***x***, then ***n* > 0**

<u>Proof</u>:

***n* = 4:** Let ***x* = 2**, so $x^2 = 2^2 = 4$. **4 > 0**

***n* = 625:** Let ***x* = 25**, so $x^2 = 25^2 = 625$. **625 > 0**

***n* = 900:** Let ***x* = -30**, so $x^2 = -30^2 = 900$. **900 > 0**

∴ If $n = x^2$ for some integer ***x***, then ***n* > 0**

Is this true for every ***n***?
A proof must handle every possible scenario.

Proof by Exhaustion Non-Example

Prove that if ***n*** has the form x^2 for some integer, ***x***, then ***n* > 0**

Proof:

***n* = 4:** Let ***x* = 2**, so $x^2 = 2^2 = 4$. **4 > 0**

***n* = 625:** Let ***x* = 25**, so $x^2 = 25^2 = 625$. **625 > 0**

***n* = 900:** Let ***x* = -30**, so $x^2 = -30^2 = 900$. **900 > 0**

∴ If $n = x^2$ for some integer ***x***, then ***n* > 0**

Is this true for every ***n***?
A proof must handle every possible scenario.

Proof by Cases

When proving something exhaustively, we can break up the domain into a finite number of cases instead of considering each possible value individually

These cases must be exhaustive (consider the **entire domain**)

Overlap in cases is OK but may introduce redundant work

- For the domain of integers could consider $n \geq 0$, $n = 0$, and $n \leq 0$
- **Better option:** $n \geq 0$ and $n < 0$ or $n > 0$ and $n \leq 0$

Non-exhaustive cases leave possibility for error

- n is positive, and n is negative are non-exaustive (missing case where $n = 0$)

Outline

- Logical Reasoning
- **Introduction to Mathematical Proofs**
  - Terminology
  - Proof by Exhaustion
  - **Disproof by Counterexample**
  - Direct Proofs
  - Proof by Contraposition
  - Proof by Contradiction

Disproof by Counterexample

How can we prove a statement is false?

Disproof by Counterexample

How can we prove a statement is false?

The theorems we try to prove are generally universally quantified implications…so we can disprove them by finding a counterexample

Disproof by Counterexample

How can we prove a statement is false?

The theorems we try to prove are generally universally quantified implications…so we can disprove them by finding a counterexample

ie: We can prove $\forall x, (P(x) \rightarrow Q(x))$ is false by finding a counterexample

This is a value for x, where $P(x)$ is TRUE, and $Q(x)$ is FALSE ($T \rightarrow F \equiv F$)

Disproof by Counterexample

Find counterexamples for each of the below statements

- Every month of the year has 30 or 31 days
- If n is an integer and n^2 is divisible by 4, then n is divisible by 4
- For every positive integer x, $x^3 < 2x$
- Every positive integer can be expressed as the sum of the squares of two integers
- Every real number has a multiplicative inverse ($xy = 1$)

Outline

- Logical Reasoning
- **Introduction to Mathematical Proofs**
  - Terminology
  - Proof by Exhaustion
  - Disproof by Counterexample
  - **Direct Proofs**
  - Proof by Contraposition
  - Proof by Contradiction

Direct Proofs

A **direct proof** for $P(x) \rightarrow Q(x)$ starts by assuming $P(x)$ as fact, and finishes by establishing $Q(x)$

It makes use of axioms, previously proven theorems, inference rules, etc

Same approach as proving a logical argument is valid

- $P(x)$ is the hypothesis
- $Q(x)$ is the conclusion

Direct Proof Example

Prove that if n is an odd integer, then n^2 is also odd

Decomposition of the Statement

- The domain of x is all integers
- $P(x)$: x is an odd integer
- $Q(x)$: x^2 is an odd integer

Direct Proof Example

Prove that if n is an odd integer, then n^2 is also odd

Proof

Assume $P(n)$ is TRUE (n is an odd integer)

There exists an integer k s.t. $n = 2k + 1$

So, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Since k is an integer, $2k^2 + 2k$ is also an integer (call it j)

So n^2 has the form $2j + 1$

Therefore n^2 is an odd integer

Direct Proof Example

Prove that if ***n*** is an odd integer, then **(*n* + 3) / 2** is an integer

Decomposition of the Statement

- The domain of ***x*** is all integers
- ***P*(*x*): *x*** is an odd integer
- ***Q*(*x*): (*x* + 3) / 2** is an odd integer

Direct Proof Example

Prove that if n is an odd integer, then **(n + 3) / 2** is an integer

Proof

Assume ***P*(*n*)** is TRUE (***n*** is an odd integer)

There exists an integer ***k*** s.t. $n = 2k + 1$

So, $n + 3 = (2k + 1) + 3 = 2k + 4 = 2\ (k + 2)$

Then $(n + 3) / 2 = (2\ (k + 2)) / 2 = k + 2$, which is an integer

Therefore $(n + 3) / 2$ is an integer

Outline

- Logical Reasoning
- **Introduction to Mathematical Proofs**
  - Terminology
  - Proof by Exhaustion
  - Disproof by Counterexample
  - Direct Proofs
  - **Proof by Contraposition**
  - Proof by Contradiction
  - Proof Examples

Proof by Contraposition

A **proof by contraposition** for $P(x) \rightarrow Q(x)$ is a proof where you:

1. Write a direct proof for $\neg Q(x) \rightarrow \neg P(x)$
2. Conclude that the contrapositive, $P(x) \rightarrow Q(x)$, is also true

Proof Layout:

Assume $\neg Q(x)$

Perform your derivations (using theorems, axioms, etc)

$\therefore \neg P(x)$

Since $\neg Q(x) \rightarrow \neg P(x)$ is TRUE, we may conclude that our original statement $P(x) \rightarrow Q(x)$ is also TRUE

Proof by Contraposition Example

Prove that if ***n*** is an integer, and **3*n* + 2** is odd, then ***n*** is odd

Decomposition of the Statement

- The domain of ***x*** is all integers
- ***P*(*x*): 3*x* + 2** is an odd integer
- ***Q*(*x*): *x*** is an odd integer

Proof by Contraposition Example

Prove that if ***n*** is an integer, and **3*n* + 2** is odd, then ***n*** is odd

<u>Proof by Contraposition</u>

Assume ***n*** is not an odd integer. So ***n*** is even.

There exists an integer ***k*** s.t. $n = 2k$

So, $3n + 2 = 3\,(2k) + 2 = 6k + 2 = 2\,(3k + 1)$

Since ***k*** is an integer, **3*k* + 1** is also an integer (call it ***j***)

Therefore, **3*n* + 2** has the form **2*j*** which means it is an even integer (not odd).

Thus, $\neg Q(x) \rightarrow \neg P(x)$

$\therefore P(x) \rightarrow Q(x)$

Outline

- Logical Reasoning
- **Introduction to Mathematical Proofs**
  - Terminology
  - Proof by Exhaustion
  - Disproof by Counterexample
  - Direct Proofs
  - Proof by Contraposition
  - **Proof by Contradiction**

Proof by Contradiction

Note that ***p*** is logically equivalent to $\neg p \rightarrow (r \wedge \neg r)$

A **proof by contradiction** for ***p*** is actually a proof for $\neg p \rightarrow (r \wedge \neg r)$ where you:

1. Write a proof starting with the asumption $\neg p$
2. Find some proposition ***r*** where you can derive both ***r*** and $\neg r$ to be TRUE (a contradiction)

Proof Layout:
Assume $\neg p$
Find something that breaks
∴ contradiction, so ***p*** has to be true

Proof by Contradiction Example

Prove that $\sqrt{2}$ is not a rational number

Decomposition of the Statement

- The domain of ***x*** is all rational numbers
- ***P***: $\forall x, x \neq \sqrt{2}$

Proof by Contradiction Example

Prove that $\sqrt{2}$ is not a rational number

Proof by Contradiction

Assume that ***r*** is a rational number and ***r*** = $\sqrt{2}$

Proof by Contradiction Example

Prove that √2 is not a rational number

Proof by Contradiction

Assume that ***r*** is a rational number and ***r*** = **√2**

There exists integers ***a*, *b*** s.t. ***r* = *a*/*b***

WLOG, we assume that ***a*** and ***b*** have no common divisors

Then $\mathbf{2 = r^2 = (a/b)^2 = a^2 / b^2}$

Proof by Contradiction Example

Prove that √2 is not a rational number

Proof by Contradiction

Assume that r is a rational number and $r = \sqrt{2}$

There exists integers a, b s.t. $r = a/b$

WLOG, we assume that a and b have no common divisors

Then $2 = r^2 = (a/b)^2 = a^2 / b^2$

Since $2 = a^2 / b^2$, $a^2 = 2b^2$, therefore a^2 is an even number, therefore a is also even

So there exists integer i s.t. $a = 2i$

Plug into $a^2 = 2b^2$ to get $4i^2 = 2b^2$ so $b^2 = 2i^2$ and we can conclude b is even

Proof by Contradiction Example

Prove that √2 is not a rational number

Proof by Contradiction
Assume that r is a rational number and $r = \sqrt{2}$

There exists integers a, b s.t. $r = a/b$
WLOG, we assume that a and b have no common divisors
Then $2 = r^2 = (a/b)^2 = a^2 / b^2$

Since $2 = a^2 / b^2$, $a^2 = 2b^2$, therefore a^2 is an even number, therefore a is also even
So there exists integer i s.t. $a = 2i$
Plug into $a^2 = 2b^2$ to get $4i^2 = 2b^2$ so $b^2 = 2i^2$ and we can conclude b is even

Since a and b are both even, they share a common divisor, 2. This is a contradiction
Therefore our original assumption is false, so no rational number = √2

Proof by Contradiction Example

Prove that √2 is not a rational number

Proof by Contradiction

Assume that ***r*** is a rational number and ***r*** = **√2**

There exists integers ***a***, ***b*** s.t. ***r* = *a*/*b***

WLOG, we **assume that *a* and *b* have no common divisors**

Then $\mathbf{2} = r^2 = (a/b)^2 = a^2 / b^2$

Since $\mathbf{2} = a^2 / b^2$, $a^2 = 2b^2$, therefore a^2 is an even number, therefore ***a*** is also even

So there exists integer ***i*** s.t. ***a* = 2*i***

Plug into $a^2 = 2b^2$ to get $4i^2 = 2b^2$ so $b^2 = 2i^2$ and we can conclude ***b*** is even

Since *a* and *b* are both even, they share a common divisor, 2. This is a contradiction

Therefore our original assumption is false, so no rational number = √2

WLOG: Without Loss of Generality

In the previous example when we say **WLOG (without loss of generality):**

- We are saying we can consider a reduced fraction without losing the generality of our argument
- We can say WLOG when conidering another case would be redundant
    - Suppose we didn't assume a and b had no common divisors
    - The first step of our proof could have been to reduce a/b to lowest terms and proceed. So instead we just say WLOG.

Proof by Contradiction Example

A **prime number** is a an integer > 1, whose only divisors are 1 and itself.

The first few prime numbers: 2, 3, 5, 7, 11, 13, 17 …

At the beginning, prime numbers are **dense**

- There are 168 between 1 and 1000 (~17%)

As we get bigger the prime numbers get more **sparse**

- There are 78,498 primes between 1 and 1,000,000 (~8%)

Theorem: There are infinitely many prime numbers

Assume that there are only finitely many primes, $p_1, p_2, p_3, \ldots, p_n$

Consider the number $Q = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$

Is Q a prime number?

- For each i, $1 \leq i \leq n$, $Q > p_i$
- By our assumption, $p_1, p_2, p_3, \ldots, p_n$ are all of the prime numbers
- Therefore Q is not prime

If Q is not prime, it must have a prime factor

- So one of p_i must be a factor of Q
- But Q divided by each p_i has a remainder of 1
- So no p_i divides Q
- So Q is a prime number

∴ Contradiction, so our original assumption is false.

Proof by contradiction that there are infinitely many prime numbers (Euclid 325 - 265 BC)

Assume that there are only finitely many primes, $p_1, p_2, p_3, \ldots, p_n$

Consider the number $Q = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$

Is Q a prime number?

For each i, $1 \leq i \leq n$, $Q > p_i$

By our assumption, $p_1, p_2, p_3, \ldots, p_n$ are all of the prime numbers

Therefore *Q* is not prime

If Q is not prime, it must have a prime factor

So one of p_i must be a factor of Q

But Q divided by each p_i has a remainder of 1

So no p_i divides Q

So *Q* is a prime number

∴ Contradiction, so our original assumption is false.

Proof by contradiction that there are infinitely many prime numbers (Euclid 325 - 265 BC)