Discrete Mathematics and Its Applications

Lecture 1: The Foundations: Logic and Proofs (1.6-1.8)

MING GAO

DASE @ ECNU
(for course related communications)
mgao@dase.ecnu.edu.cn

Sep. 20, 2018

Outline

Argument

Definition

An *argument* in propositional logic is a sequence of propositions. All but the final proposition in the argument are called *premises* or *hypotheses* and the final proposition is called the *conclusion*.

Argument

Definition

An *argument* in propositional logic is a sequence of propositions. All but the final proposition in the argument are called *premises* or *hypotheses* and the final proposition is called the *conclusion*.

Form

Given

- Hypothesis 1
- Hypothesis 2
- $\cdots$
- Hypothesis n

Then:

- Conclusion

Valid argument

Definition

We say that the statement is *valid* if when all hypotheses are true, the conclusion must be true as well.
In that case, we say that the conclusion logically follows from the hypotheses.

Valid argument

Definition

We say that the statement is *valid* if when all hypotheses are true, the conclusion must be true as well.
In that case, we say that the conclusion logically follows from the hypotheses.

Form

More precisely, to show that conclusion q logically follows from hypotheses $p_1, p_2, \cdots, p_n$, we need to show that

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \rightarrow q$$

is always true, i.e., is a tautology.
That is

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \Rightarrow q$$

An example

Consider the following argument:

- Hypotheses: p and $p \rightarrow q$
- Conclusion: q

Is this a valid argument?

An example

Consider the following argument:

- Hypotheses: p and $p \to q$
- Conclusion: q

Is this a valid argument?

It is valid!

The argument is in the form of $(p \land (p \to q)) \to q$.
Its validity can be seen from the following truth table

p	q	$p \to q$	$p \land (p \to q)$	$(p \land (p \to q)) \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

An example

Consider the following argument:

- Hypotheses: p and $p \to q$
- Conclusion: q

Is this a valid argument?

An example

Consider the following argument:

- Hypotheses: p and $p \rightarrow q$
- Conclusion: q

Is this a valid argument?

It is valid!

The argument is in the form of $(p \wedge (p \rightarrow q)) \rightarrow q$.
Its validity can also be seen from the propositional equivalence

$$\begin{aligned}(p \wedge (p \rightarrow q)) \rightarrow q &\equiv \neg(p \wedge (\neg p \vee q)) \vee q \\ &\equiv \neg((p \wedge \neg p) \vee (p \wedge q)) \vee q \\ &\equiv \neg(p \wedge q) \vee q \\ &\equiv \neg p \vee \neg q \vee q \equiv T\end{aligned}$$

Thus, we have $(p \wedge (p \rightarrow q)) \Rightarrow q$.

An example

Consider the following argument:

- Hypotheses: p and $p \to q$
- Conclusion: q

Is this a valid argument?

An example

Consider the following argument:

- Hypotheses: p and $p \to q$
- Conclusion: q

Is this a valid argument?

It is valid!

The argument is in the form of $(p \land (p \to q)) \to q$.
Its validity can also be seen from the following inference

Steps	**Reasons**

An example

Consider the following argument:

- Hypotheses: p and $p \to q$
- Conclusion: q

Is this a valid argument?

It is valid!

The argument is in the form of $(p \wedge (p \to q)) \to q$.
Its validity can also be seen from the following inference

Steps	Reasons
1. p is true	Hypothesis

An example

Consider the following argument:

- Hypotheses: p and $p \to q$
- Conclusion: q

Is this a valid argument?

It is valid!

The argument is in the form of $(p \wedge (p \to q)) \to q$.
Its validity can also be seen from the following inference

Steps	Reasons
1. p is true	Hypothesis
2. $p \to q$ is true	Hypothesis

An example

Consider the following argument:

- Hypotheses: p and $p \to q$
- Conclusion: q

Is this a valid argument?

It is valid!

The argument is in the form of $(p \wedge (p \to q)) \to q$.

Its validity can also be seen from the following inference

Steps	**Reasons**
1. p is true	Hypothesis
2. $p \to q$ is true	Hypothesis
3. q is true	Property of implication

Thus, we have $(p \wedge (p \to q)) \to q$.

Modus ponens

The previous truth table that we can use in our argument is extremely useful when making arguments. It is called *Modus ponens*, and is one of many useful rules of inference.

Modus ponens

The previous truth table that we can use in our argument is extremely useful when making arguments. It is called *Modus ponens*, and is one of many useful rules of inference.

Modus ponens

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

Modus ponens

The previous truth table that we can use in our argument is extremely useful when making arguments. It is called *Modus ponens*, and is one of many useful rules of inference.

Modus ponens

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

- In particular, modus ponens tells us that if a conditional statement and the hypothesis of this conditional statement are both true, then the conclusion must also be true.

Modus ponens

The previous truth table that we can use in our argument is extremely useful when making arguments. It is called *Modus ponens*, and is one of many useful rules of inference.

Modus ponens

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

- In particular, modus ponens tells us that if a conditional statement and the hypothesis of this conditional statement are both true, then the conclusion must also be true.
- However, a valid argument may lead to an incorrect conclusion if one or more of its hypothesis is false.

Examples

Correct conclusion

- Hypothesis: "It is snowing today"
- Conditional statement: "If it snows today, then we will go skiing"

Then, by modus ponens, it follows that the conclusion of the conditional statement, "We will go skiing" is true.

Examples

Correct conclusion

- Hypothesis: "It is snowing today"
- Conditional statement: "If it snows today, then we will go skiing"

Then, by modus ponens, it follows that the conclusion of the conditional statement, "We will go skiing" is true.

Undetermined conclusion

- Hypothesis: "You do not work hard";
- Conditional statement: "If you work hard, then you will get A from this course".

Then, whether will you get A from this course?

Inference rules

Modus ponens

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

$(p \wedge (p \rightarrow q)) \rightarrow q$

Inference rules

Modus ponens

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

$(p \wedge (p \rightarrow q)) \rightarrow q$

Modus tollens

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

$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$

Inference rules

Modus ponens

$$\begin{array}{l} \quad p \\ \quad p \to q \\ \hline \therefore q \end{array}$$

$(p \land (p \to q)) \to q$

Modus tollens

$$\begin{array}{l} \quad \neg q \\ \quad p \to q \\ \hline \therefore \neg p \end{array}$$

$(\neg q \land (p \to q)) \to \neg p$

Hypothetical syllogism

$$\begin{array}{l} \quad p \to q \\ \quad q \to r \\ \hline \therefore p \to r \end{array}$$

$((p \to q) \land (q \to r)) \to (p \to r)$

Inference rules

Modus ponens

$$\begin{array}{l} \quad p \\ \quad p \to q \\ \hline \therefore q \end{array}$$

$(p \wedge (p \to q)) \to q$

Modus tollens

$$\begin{array}{l} \quad \neg q \\ \quad p \to q \\ \hline \therefore \neg p \end{array}$$

$(\neg q \wedge (p \to q)) \to \neg p$

Hypothetical syllogism

$$\begin{array}{l} \quad p \to q \\ \quad q \to r \\ \hline \therefore p \to r \end{array}$$

$((p \to q) \wedge (q \to r)) \to (p \to r)$

Disjunction syllogism

$$\begin{array}{l} \quad p \vee q \\ \quad \neg p \\ \hline \therefore q \end{array}$$

$(p \vee q) \wedge \neg p \to q$

Inference rules Cont'd

Addition

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

$$p \rightarrow p \vee q$$

Inference rules Cont'd

Addition

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

$p \rightarrow p \vee q$

Simplification

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

$p \wedge q \rightarrow p$

Inference rules Cont'd

Addition

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

$p \rightarrow p \vee q$

Simplification

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

$p \wedge q \rightarrow p$

Conjunction

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

$p \wedge q \rightarrow p \wedge q$

Inference rules Cont'd

Addition

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

$p \rightarrow p \vee q$

Simplification

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

$p \wedge q \rightarrow p$

Conjunction

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

$p \wedge q \rightarrow p \wedge q$

Resolution

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

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof of resolution law

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof of resolution law

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

$(p \lor q) \land (\neg p \lor r) \rightarrow (q \lor r)$

Proof I

Steps	Reasons

Proof of resolution law

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

$(p \lor q) \land (\neg p \lor r) \rightarrow (q \lor r)$

Proof I

Steps	Reasons
1. $p \lor q$ is true	Hypothesis

Proof of resolution law

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof I

Steps	Reasons
1. $p \vee q$ is true	Hypothesis
2. $\neg q \rightarrow p$ is true	Equivalent to Step 1

Proof of resolution law

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

$(p \lor q) \land (\neg p \lor r) \to (q \lor r)$

Proof I

Steps	**Reasons**
1. $p \lor q$ is true	Hypothesis
2. $\neg q \to p$ is true	Equivalent to Step 1
3. $\neg p \lor r$ is true	Hypothesis

Proof of resolution law

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

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof I

Steps	**Reasons**
1. $p \vee q$ is true	Hypothesis
2. $\neg q \rightarrow p$ is true	Equivalent to Step 1
3. $\neg p \vee r$ is true	Hypothesis
4. $p \rightarrow r$ is true	Equivalent to Step 3

Proof of resolution law

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof I

Steps	Reasons
1. $p \vee q$ is true	Hypothesis
2. $\neg q \rightarrow p$ is true	Equivalent to Step 1
3. $\neg p \vee r$ is true	Hypothesis
4. $p \rightarrow r$ is true	Equivalent to Step 3
5. $\neg q \rightarrow r$	Hypothetical syllogism w.r.t. Steps 2 and 4

Proof of resolution law

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof I

Steps	Reasons
1. $p \vee q$ is true	Hypothesis
2. $\neg q \rightarrow p$ is true	Equivalent to Step 1
3. $\neg p \vee r$ is true	Hypothesis
4. $p \rightarrow r$ is true	Equivalent to Step 3
5. $\neg q \rightarrow r$	Hypothetical syllogism w.r.t. Steps 2 and 4
6. $q \vee r$	Equivalent to Step 5

Proof of resolution law

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \to (q \vee r)$

Proof of resolution law

$$\begin{array}{r} p \lor q \\ \neg p \lor r \\ \hline \therefore q \lor r \end{array}$$

$$(p \lor q) \land (\neg p \lor r) \to (q \lor r)$$

Proof II

Steps	**Reasons**

Proof of resolution law

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof II

Steps	Reasons
1. $\neg q$ is true	Additional hypothesis

Proof of resolution law

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

$(p \vee q) \wedge (\neg p \vee r) \to (q \vee r)$

Proof II

Steps	**Reasons**
1. $\neg q$ is true	Additional hypothesis
2. $p \vee q$ is true	Equivalent to Step 1

Proof of resolution law

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

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof II

Steps	Reasons
1. $\neg q$ is true	Additional hypothesis
2. $p \vee q$ is true	Equivalent to Step 1
3. $\neg(\neg q) \vee p$ is true	Equivalent to Step 2

Proof of resolution law

$$\begin{array}{r} p \lor q \\ \neg p \lor r \\ \hline \therefore q \lor r \end{array}$$

$(p \lor q) \land (\neg p \lor r) \to (q \lor r)$

Proof II

Steps	**Reasons**
1. $\neg q$ is true	Additional hypothesis
2. $p \lor q$ is true	Equivalent to Step 1
3. $\neg(\neg q) \lor p$ is true	Equivalent to Step 2
4. $\neg q \to p$ is true	Equivalent to Step 3

Proof of resolution law

$$\begin{array}{r} p \lor q \\ \neg p \lor r \\ \hline \therefore q \lor r \end{array}$$

$(p \lor q) \land (\neg p \lor r) \to (q \lor r)$

Proof II

Steps	Reasons
1. $\neg q$ is true	Additional hypothesis
2. $p \lor q$ is true	Equivalent to Step 1
3. $\neg(\neg q) \lor p$ is true	Equivalent to Step 2
4. $\neg q \to p$ is true	Equivalent to Step 3
5. p is true	Modus ponens w.r.t. Steps 1 and 4

Proof of resolution law

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof II

Steps	Reasons
1. $\neg q$ is true	Additional hypothesis
2. $p \vee q$ is true	Equivalent to Step 1
3. $\neg(\neg q) \vee p$ is true	Equivalent to Step 2
4. $\neg q \rightarrow p$ is true	Equivalent to Step 3
5. p is true	Modus ponens w.r.t. Steps 1 and 4
6. $\neg p \vee r$ is true	hypothesis

Proof of resolution law

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof II

Steps	Reasons
1. $\neg q$ is true	Additional hypothesis
2. $p \vee q$ is true	Equivalent to Step 1
3. $\neg(\neg q) \vee p$ is true	Equivalent to Step 2
4. $\neg q \rightarrow p$ is true	Equivalent to Step 3
5. p is true	Modus ponens w.r.t. Steps 1 and 4
6. $\neg p \vee r$ is true	hypothesis
7. $p \rightarrow r$ is true	Equivalent to Step 6

Proof of resolution law

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Proof II

Steps	Reasons
1. $\neg q$ is true	Additional hypothesis
2. $p \vee q$ is true	Equivalent to Step 1
3. $\neg(\neg q) \vee p$ is true	Equivalent to Step 2
4. $\neg q \rightarrow p$ is true	Equivalent to Step 3
5. p is true	Modus ponens w.r.t. Steps 1 and 4
6. $\neg p \vee r$ is true	hypothesis
7. $p \rightarrow r$ is true	Equivalent to Step 6
8. r is true	Modus ponens w.r.t. Steps 5 and 7

What do you find?

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

What do you find?

$$\begin{array}{r} p \lor q \\ \neg p \lor r \\ \hline \therefore q \lor r \end{array}$$

$(p \lor q) \land (\neg p \lor r) \to (q \lor r)$

Truth table

p	q	r	$p \lor q$	$\neg p \lor r$	$(p \lor q) \land (\neg p \lor r)$	$q \lor r$
T	T	T	T	T	T	T
T	T	F	T	F	F	T
T	F	T	T	T	T	T
T	F	F	T	F	F	F
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T	F	T
F	F	F	F	T	F	F

What do you find?

$$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

$(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$

Truth table

p	q	r	$p \vee q$	$\neg p \vee r$	$(p \vee q) \wedge (\neg p \vee r)$	$q \vee r$
T	T	T	T	T	T	T
T	T	F	T	F	F	T
T	F	T	T	T	T	T
T	F	F	T	F	F	F
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T	F	T
F	F	F	F	T	F	F

That is $(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$, and $(p \vee q) \wedge (\neg p \vee r) \not\Rightarrow (q \vee r)$.

Using inference rules

Argue that $p \rightarrow q$, $(p \vee r)$, and $\neg r$ logically leads to the conclusion q.

Using inference rules

Argue that $p \to q$, $(p \vee r)$, and $\neg r$ logically leads to the conclusion q.

Steps	**Reasons**

Using inference rules

Argue that $p \to q$, $(p \vee r)$, and $\neg r$ logically leads to the conclusion q.

Steps	**Reasons**
1. $p \vee r$ is true	Hypothesis

Using inference rules

Argue that $p \to q$, $(p \vee r)$, and $\neg r$ logically leads to the conclusion q.

Steps	**Reasons**
1. $p \vee r$ is true	Hypothesis
2. $\neg r$ is true	Hypothesis

Using inference rules

Argue that $p \to q$, $(p \vee r)$, and $\neg r$ logically leads to the conclusion q.

Steps	Reasons
1. $p \vee r$ is true	Hypothesis
2. $\neg r$ is true	Hypothesis
3. p is true	Disjunctive syllogism using Step 1 and 2

Using inference rules

Argue that $p \to q$, $(p \vee r)$, and $\neg r$ logically leads to the conclusion q.

Steps	**Reasons**
1. $p \vee r$ is true	Hypothesis
2. $\neg r$ is true	Hypothesis
3. p is true	Disjunctive syllogism using Step 1 and 2
4. $p \to q$ is true	Hypothesis

Using inference rules

Argue that $p \rightarrow q$, $(p \vee r)$, and $\neg r$ logically leads to the conclusion q.

Steps	Reasons
1. $p \vee r$ is true	Hypothesis
2. $\neg r$ is true	Hypothesis
3. p is true	Disjunctive syllogism using Step 1 and 2
4. $p \rightarrow q$ is true	Hypothesis
5. q is true	Modus ponens using Step 3 and 4.

Another example

Argue that $p \rightarrow r$ and $q \rightarrow r$ logically leads to the conclusion $(p \vee q) \rightarrow r$.

Another example

Argue that $p \to r$ and $q \to r$ logically leads to the conclusion $(p \vee q) \to r$.

Steps	Reasons

Another example

Argue that $p \to r$ and $q \to r$ logically leads to the conclusion $(p \vee q) \to r$.

Steps	Reasons
1. $p \to r$	Hypothesis

Another example

Argue that $p \rightarrow r$ and $q \rightarrow r$ logically leads to the conclusion $(p \vee q) \rightarrow r$.

Steps	**Reasons**
1. $p \rightarrow r$	Hypothesis
2. $\neg p \vee r$	Equivalence of Step 1

Another example

Argue that $p \to r$ and $q \to r$ logically leads to the conclusion $(p \vee q) \to r$.

Steps	Reasons
1. $p \to r$	Hypothesis
2. $\neg p \vee r$	Equivalence of Step 1
3. $q \to r$	Hypothesis

Another example

Argue that $p \rightarrow r$ and $q \rightarrow r$ logically leads to the conclusion $(p \vee q) \rightarrow r$.

Steps	**Reasons**
1. $p \rightarrow r$	Hypothesis
2. $\neg p \vee r$	Equivalence of Step 1
3. $q \rightarrow r$	Hypothesis
4. $\neg q \vee r$	Equivalence of Step 3

Another example

Argue that $p \to r$ and $q \to r$ logically leads to the conclusion $(p \vee q) \to r$.

Steps	**Reasons**
1. $p \to r$	Hypothesis
2. $\neg p \vee r$	Equivalence of Step 1
3. $q \to r$	Hypothesis
4. $\neg q \vee r$	Equivalence of Step 3
5. $(\neg p \vee r) \wedge (\neg q \vee r)$	Conjunction of Steps 2 and 4.

Another example

Argue that $p \to r$ and $q \to r$ logically leads to the conclusion $(p \vee q) \to r$.

Steps	**Reasons**
1. $p \to r$	Hypothesis
2. $\neg p \vee r$	Equivalence of Step 1
3. $q \to r$	Hypothesis
4. $\neg q \vee r$	Equivalence of Step 3
5. $(\neg p \vee r) \wedge (\neg q \vee r)$	Conjunction of Steps 2 and 4.
6. ... (left as homework)	

Inference rules for quantified statements

Universal instantiation

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Inference rules for quantified statements

Universal instantiation

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Universal generalization

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Inference rules for quantified statements

Universal instantiation

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Universal generalization

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Existential instantiation

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element}}$$

Inference rules for quantified statements

Universal instantiation

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Universal generalization

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Existential instantiation

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element}}$$

Existential generalization

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(c)}$$

An example

Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."

- $C(x)$: "x is in this class";
- $B(x)$: "x has read the book";
- $P(x)$: "x passed the first exam".

An example

Show that the premises “A student in this class has not read the book,” and “Everyone in this class passed the first exam” imply the conclusion “Someone who passed the first exam has not read the book.”

- $C(x)$: “x is in this class”;
- $B(x)$: “x has read the book”;
- $P(x)$: “x passed the first exam”.

Therefore the premises and conclusion of the argument can be listed as follows:

An example

Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."

- $C(x)$: "x is in this class";
- $B(x)$: "x has read the book";
- $P(x)$: "x passed the first exam".

Therefore the premises and conclusion of the argument can be listed as follows:

- Premises: $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;

An example

Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."

- $C(x)$: "x is in this class";
- $B(x)$: "x has read the book";
- $P(x)$: "x passed the first exam".

Therefore the premises and conclusion of the argument can be listed as follows:

- Premises: $\exists x(C(x) \land \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \land \neg B(x))$.

An example Cont'd

Inference

- Premises: $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \wedge \neg B(x))$

These steps can establish the conclusion from the premises.

An example Cont'd

Inference

- Premises: $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \wedge \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	Reasons

An example Cont'd

Inference

- Premises: $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \wedge \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	**Reasons**
1. $\exists x(C(x) \wedge \neg B(x))$ is true	Premise

An example Cont'd

Inference

- Premises: $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \wedge \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	**Reasons**
1. $\exists x(C(x) \wedge \neg B(x))$ is true	Premise
2. $C(a) \wedge \neg B(a)$ is true	Existential instantiation from (1)

An example Cont'd

Inference

- Premises: $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \wedge \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	**Reasons**
1. $\exists x(C(x) \wedge \neg B(x))$ is true	Premise
2. $C(a) \wedge \neg B(a)$ is true	Existential instantiation from (1)
3. $C(a)$ is true	Simplification from (2)

An example Cont'd

Inference

- Premises: $\exists x(C(x) \land \neg B(x))$ and $\forall x(C(x) \to P(x))$;
- Conclusion: $\exists x(P(x) \land \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	Reasons
1. $\exists x(C(x) \land \neg B(x))$ is true	Premise
2. $C(a) \land \neg B(a)$ is true	Existential instantiation from (1)
3. $C(a)$ is true	Simplification from (2)
4. $\forall x(C(x) \to P(x))$ is true	Premise

An example Cont'd

Inference

- Premises: $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \wedge \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	**Reasons**
1. $\exists x(C(x) \wedge \neg B(x))$ is true	Premise
2. $C(a) \wedge \neg B(a)$ is true	Existential instantiation from (1)
3. $C(a)$ is true	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$ is true	Premise
5. $C(a) \rightarrow P(a)$ is true	Universal instantiation from (4)

An example Cont'd

Inference

- Premises: $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \wedge \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	Reasons
1. $\exists x(C(x) \wedge \neg B(x))$ is true	Premise
2. $C(a) \wedge \neg B(a)$ is true	Existential instantiation from (1)
3. $C(a)$ is true	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$ is true	Premise
5. $C(a) \rightarrow P(a)$ is true	Universal instantiation from (4)
6. $P(a)$ is true	Modus ponens from (3) and (5)

An example Cont'd

Inference

- Premises: $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \wedge \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	**Reasons**
1. $\exists x(C(x) \wedge \neg B(x))$ is true	Premise
2. $C(a) \wedge \neg B(a)$ is true	Existential instantiation from (1)
3. $C(a)$ is true	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$ is true	Premise
5. $C(a) \rightarrow P(a)$ is true	Universal instantiation from (4)
6. $P(a)$ is true	Modus ponens from (3) and (5)
7. $\neg B(a)$ is true	Simplification from (2)

An example Cont'd

Inference

- Premises: $\exists x(C(x) \land \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$;
- Conclusion: $\exists x(P(x) \land \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	**Reasons**
1. $\exists x(C(x) \land \neg B(x))$ is true	Premise
2. $C(a) \land \neg B(a)$ is true	Existential instantiation from (1)
3. $C(a)$ is true	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$ is true	Premise
5. $C(a) \rightarrow P(a)$ is true	Universal instantiation from (4)
6. $P(a)$ is true	Modus ponens from (3) and (5)
7. $\neg B(a)$ is true	Simplification from (2)
8. $P(a) \land \neg B(a)$ is true	Conjunction from (6) and (7)

An example Cont'd

Inference

- Premises: $\exists x(C(x) \land \neg B(x))$ and $\forall x(C(x) \to P(x))$;
- Conclusion: $\exists x(P(x) \land \neg B(x))$

These steps can establish the conclusion from the premises.

Steps	**Reasons**
1. $\exists x(C(x) \land \neg B(x))$ is true	Premise
2. $C(a) \land \neg B(a)$ is true	Existential instantiation from (1)
3. $C(a)$ is true	Simplification from (2)
4. $\forall x(C(x) \to P(x))$ is true	Premise
5. $C(a) \to P(a)$ is true	Universal instantiation from (4)
6. $P(a)$ is true	Modus ponens from (3) and (5)
7. $\neg B(a)$ is true	Simplification from (2)
8. $P(a) \land \neg B(a)$ is true	Conjunction from (6) and (7)
9. $\exists x(P(x) \land \neg B(x))$ is true	Existential generalization from (8)

Motivation

Using inference rules, we can prove facts in propositional logic. However, in many cases, we want to prove wider range of mathematical facts. Inference rules play crucial parts in providing high-level structures for our proofs.

Motivation

Using inference rules, we can prove facts in propositional logic. However, in many cases, we want to prove wider range of mathematical facts. Inference rules play crucial parts in providing high-level structures for our proofs.

In this lecture, we will focus on two general proof techniques that originate from five simple inference rules.

- Direct proofs
- Proofs by contraposition
- Proofs by contradiction
- Proofs by cases
- Mathematical induction

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.
- An **axiom** is a statement that is assumed to be true. (Note that we do not prove an axiom; therefore, the validity of a theorem proved using an axiom relies of the validity of the axiom.)

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.
- An **axiom** is a statement that is assumed to be true. (Note that we do not prove an axiom; therefore, the validity of a theorem proved using an axiom relies of the validity of the axiom.)
- To prove a theorem, we may prove many simple lemmas to make our argument. A **lemma**, in this sense, is a smaller theorem (or a supportive one).

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.
- An **axiom** is a statement that is assumed to be true. (Note that we do not prove an axiom; therefore, the validity of a theorem proved using an axiom relies of the validity of the axiom.)
- To prove a theorem, we may prove many simple lemmas to make our argument. A **lemma**, in this sense, is a smaller theorem (or a supportive one).
- A **corollary** is a theorem which is a "fairly" direct result of other theorems.

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.
- An **axiom** is a statement that is assumed to be true. (Note that we do not prove an axiom; therefore, the validity of a theorem proved using an axiom relies of the validity of the axiom.)
- To prove a theorem, we may prove many simple lemmas to make our argument. A **lemma**, in this sense, is a smaller theorem (or a supportive one).
- A **corollary** is a theorem which is a "fairly" direct result of other theorems.
- A **conjecture** is a statement which we do not know if it is true or false.

Not easy to prove

Fermat's Last Theorem

Theorem: No three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ when $n > 2$.

Not easy to prove

Fermat's Last Theorem

Theorem: No three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ when $n > 2$.

This theorem has been conjectured by Pierre de Fermat in 1637. It remained a conjecture until Andrew Wiles proved it in 1994.

Not easy to prove

Fermat's Last Theorem

Theorem: No three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ when $n > 2$.

This theorem has been conjectured by Pierre de Fermat in 1637. It remained a conjecture until Andrew Wiles proved it in 1994.

Goldbach's conjecture

Conjecture: Every even integer greater than 2 can be expressed as the sum of two primes.

Not easy to prove

Fermat's Last Theorem

Theorem: No three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ when $n > 2$.

This theorem has been conjectured by Pierre de Fermat in 1637. It remained a conjecture until Andrew Wiles proved it in 1994.

Goldbach's conjecture

Conjecture: Every even integer greater than 2 can be expressed as the sum of two primes.

In 1742, Christian Goldbach proposed this cojecture to Leonhard Euler. It remains unsolved.

Direct proofs

When we want to prove a theorem of the form $p \to q$, we can assume that p is true, then use this to argue that q has to be true as well.

Direct proofs

Theorem:

$p \to q$.

Proof.

Assume p.

...

(then show that q follows from p) $\square$

Example 1

Theorem

If x is an even number, then x^2 is an even number.

Example 1

Theorem

If x is an even number, then x^2 is an even number.

Proof.

Assume that x is an even number.

Example 1

Theorem

If x is an even number, then x^2 is an even number.

Proof.

Assume that x is an even number.
By definition, there exists an integer k such that $x = 2k$.

Example 1

Theorem

If x is an even number, then x^2 is an even number.

Proof.

Assume that x is an even number.
By definition, there exists an integer k such that $x = 2k$. This implies that $x^2 = (2k)^2 = 4k^2$.

Example 1

Theorem

If x is an even number, then x^2 is an even number.

Proof.

Assume that x is an even number.

By definition, there exists an integer k such that $x = 2k$. This implies that $x^2 = (2k)^2 = 4k^2$. Since k is an integer, $2k^2$ is also an integer. Hence we can write $x^2 = 2 \cdot (2k^2)$ where $2k^2$ is an integer; this means that x^2 is even. $\square$

Example 1: disected

Theorem

$(\forall x)$ If x is an even number, then x^2 is an even number.

Example 1: disected

Theorem

$(\forall x)$ If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$: "x is an even number".

Example 1: disected

Theorem

$(\forall x)$ If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$: "x is an even number".
- By definition, $P(x) \to R(x)$, where $R(x) =$"there exists an integer k such that $x = 2k$."

Example 1: disected

Theorem

$(\forall x)$ If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$: "x is an even number".
- By definition, $P(x) \rightarrow R(x)$, where $R(x) =$"there exists an integer k such that $x = 2k$."
- $R(x) \rightarrow S(x)$, where $S(x) =$ "there exists an integer k such that $x^2 = (2k)^2 = 4k^2$."

Example 1: disected

Theorem

$(\forall x)$ If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$: "x is an even number".
- By definition, $P(x) \to R(x)$, where $R(x) =$"there exists an integer k such that $x = 2k$."
- $R(x) \to S(x)$, where $S(x) =$ "there exists an integer k such that $x^2 = (2k)^2 = 4k^2$."
- By elementary algebra, we know that U is true, where $U =$ "for all integer k, $2k^2$ is an integer."

Example 1: disected

Theorem

($\forall x$) If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$: "x is an even number".
- By definition, $P(x) \rightarrow R(x)$, where $R(x) =$"there exists an integer k such that $x = 2k$."
- $R(x) \rightarrow S(x)$, where $S(x) =$ "there exists an integer k such that $x^2 = (2k)^2 = 4k^2$."
- By elementary algebra, we know that U is true, where $U =$ "for all integer k, $2k^2$ is an integer."
- $S(x) \wedge U \rightarrow V(x)$, where $V =$ "there exists an integer k such that $x^2 = 2 \cdot (2k^2)$ where $2k^2$ is an integer."

Example 1: disected

Theorem

($\forall x$) If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$: "x is an even number".
- By definition, $P(x) \to R(x)$, where $R(x) =$"there exists an integer k such that $x = 2k$."
- $R(x) \to S(x)$, where $S(x) =$ "there exists an integer k such that $x^2 = (2k)^2 = 4k^2$."
- By elementary algebra, we know that U is true, where $U =$ "for all integer k, $2k^2$ is an integer."
- $S(x) \wedge U \to V(x)$, where $V =$ "there exists an integer k such that $x^2 = 2 \cdot (2k^2)$ where $2k^2$ is an integer."
- By definition, $V(x) \to Q(x)$, where $Q(x) =$ "x^2 is even".

Example 1: be careful

When we prove a statement with universal quantifiers like:

> $(\forall x)$ If x is an even number, then x^2 is an even number

we have to be *extremely* careful not to assume anything about x except those state explicitly in the assumption.

Practice: Back to our subgoal

Can you use direct proofs to show the following theorem?

Theorem

For any positive number n and a such that $a > \sqrt{n}$, then $n/a \leq \sqrt{n}$.

Practice: Back to our subgoal

Can you use direct proofs to show the following theorem?

Theorem

For any positive number n and a such that $a > \sqrt{n}$, then $n/a \leq \sqrt{n}$.

Proof.

Assume that $a > \sqrt{n}$.

Practice: Back to our subgoal

Can you use direct proofs to show the following theorem?

Theorem

For any positive number n and a such that $a > \sqrt{n}$, then $n/a \leq \sqrt{n}$.

Proof.

Assume that $a > \sqrt{n}$. Since

$$n = n,$$

by dividing the left side by a and the right side by $\sqrt{n}$, we get that

$$\frac{n}{a} < \frac{n}{\sqrt{n}},$$

because both a and $\sqrt{n}$ are positive. Hence, $n/a < \sqrt{n}$ as required. □

Practice: Divisibility by 3 (1)

Let's try to prove a well-known fact.

Theorem

An integer n is divisible by 3 if the sum of the digits of n is divisible by 3.

Practice: Divisibility by 3 (1)

Let's try to prove a well-known fact.

Theorem

An integer n is divisible by 3 if the sum of the digits of n is divisible by 3.

Let's start by proving this lemma.

Lemma

For any integer $k \geq 0$, $10^k - 1$ is divisible by 3.

Practice: Divisibility by 3 (2)

Proof.

Assume that the sum of the digits of n is divisible by 3. We will show that n is divisible by 3.

Let k be the number of digits of n. Let $a_1, a_2, \ldots, a_k$ be the digits of n where a_1 is the most significant digit and a_k is the least significant one. Therefore, we can write

$$n = a_1 \cdot 10^{k-1} + a_2 \cdot 10^{k-2} + \cdots + a_{k-1} \cdot 10^1 + a_k \cdot 10^0.$$

Consider the i-th term: $a_i \cdot 10^{k-i-1}$. From Lemma 5, we know that $10^{k-i-1} - 1$ is divisible by 3. Thus $a_i \cdot (10^{k-i-1} - 1)$ is also divisible by 3.

Therefore, the remainder of $a_i \cdot 10^{k-i-1}$ divided by 3 is equal to the remainder of a_i divided by 3.

Summing all terms, the remainder of the division of n by 3 is $a_1 + a_2 + \cdots + a_k$. Since 3 divides this number, the remainder of $n/3$ is 0; thus, 3 divides n. $\square$

Proof by contraposition

$$(p \to q) \Leftrightarrow (\neg q \to \neg p).$$

That is, when we want to prove a theorem of the form $p \to q$, we can prove $(\neg q \to \neg p)$ as well.

Proof by contraposition

Theorem:

$p \to q$.

Proof.

Assume $\neg q$.

...

(then show that $\neg p$ follows from $\neg q$) $\square$

Practice

Theorem

If x^2 is an even number, then x is an even number,

Practice

Theorem

If x^2 is an even number, then x is an even number,

Proof.

We will prove by contraposition. Assume that x is not an even number.

□

An incorrect proof is not a proof

Theorem

For any numbers x and y, $x = y$.

Proof.

Assume that

$$x = y.$$

Multiplying both terms by 0, we get that

$$0 \cdot x = 0 \cdot y,$$

and this implies

$$0 = 0,$$

which is clearly true. □

What is wrong with this (non) proof?

Proving iff statements

How can we prove a statement of the form $p \leftrightarrow q$? For example:

Theorem

x is an even number iff x^2 is an even number.

Proving iff statements

How can we prove a statement of the form $p \leftrightarrow q$? For example:

Theorem

x is an even number iff x^2 is an even number.

Proof.

We will prove that the statement is true in both directions.

1. $\rightarrow$ is true;
2. $\leftarrow$ is also true.

$\square$

How to be good at proving theorems?

In a way, proving theorems is like solving puzzles. There is no general rules on how to prove theorems.

But you can get better by (1) trying to read and understand good proofs and by (2) practicing.

How to be good at proving theorems?

In a way, proving theorems is like solving puzzles. There is no general rules on how to prove theorems.
But you can get better by (1) trying to read and understand good proofs and by (2) practicing.

There are many levels of understandings:

- Understand each step of the proof and how each step follows from previous ones
- Understand why the proof needs each step
- Can apply techniques or proof strategies learned from this proof for proving other statements

Proofs by contradiction

We want to prove that proposition p is true. To do so, we first assume that p is false, and show that this logically leads to a contradiction. This means that it is impossible for p to be false; hence, p has to be true. This is called a proof by contradiction or *reductio ad absurdum*.

Contradiction

Theorem:

p

Proof.

We use prove by contradiction.

Assume $\neg p$.

...

(then show that r and $\neg r$ follows from $\neg p$)

This is a contradiction. Therefore, p must be true. □

Example I

Theorem

$\sqrt{2}$ is irrational.

Proof.

We prove by contradiction. Assume that the theorem is false, i.e., assume that $\sqrt{2}$ is rational.

Example I

Theorem

$\sqrt{2}$ is irrational.

Proof.

We prove by contradiction. Assume that the theorem is false, i.e., assume that $\sqrt{2}$ is rational.
Therefore, there exists a pair of positive integers a and b such that $\sqrt{2} = a/b$.

Example I

Theorem

$\sqrt{2}$ is irrational.

Proof.

We prove by contradiction. Assume that the theorem is false, i.e., assume that $\sqrt{2}$ is rational.
Therefore, there exists a pair of positive integers a and b such that $\sqrt{2} = a/b$. Let's choose the pair a and b such that b is minimum. In this case, a and b share no common factors.

Example I

Theorem

$\sqrt{2}$ is irrational.

Proof.

We prove by contradiction. Assume that the theorem is false, i.e., assume that $\sqrt{2}$ is rational.
Therefore, there exists a pair of positive integers a and b such that $\sqrt{2} = a/b$. Let's choose the pair a and b such that b is minimum. In this case, a and b share no common factors.
Let's square both terms. We get $2 = a^2/b^2$, or

$$a^2 = 2b^2.$$

(cont. in next slide) □

Example I (2)

Proof. (cont.)

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number.

Example I (2)

Proof. (cont.)

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number.
Again by definition, there exists integer k such that $a = 2k$. We then obtain

$$2b^2 = (2k)^2 = 4k^2,$$

i.e., $b^2 = 2k^2$.

Example I (2)

Proof. (cont.)

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number.
Again by definition, there exists integer k such that $a = 2k$. We then obtain

$$2b^2 = (2k)^2 = 4k^2,$$

i.e., $b^2 = 2k^2$. This implies that b^2 is an even number. Again, this means that b must be an even number.

Example I (2)

Proof. (cont.)

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number.
Again by definition, there exists integer k such that $a = 2k$. We then obtain

$$2b^2 = (2k)^2 = 4k^2,$$

i.e., $b^2 = 2k^2$. This implies that b^2 is an even number. Again, this means that b must be an even number.

[quick check] Do you see that we are arriving at a contradiction here?

Example I (2)

Proof. (cont.)

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number.
Again by definition, there exists integer k such that $a = 2k$. We then obtain

$$2b^2 = (2k)^2 = 4k^2,$$

i.e., $b^2 = 2k^2$. This implies that b^2 is an even number. Again, this means that b must be an even number.

[quick check] Do you see that we are arriving at a contradiction here?

Since a and b are both even numbers, they share 2 as a common factor. This contradicts the fact that we choose the pair a and b that share no common factor.
Therefore, $\sqrt{2}$ must be irrational. $\square$

Proofs by cases

- The proof technique that we shall discuss is closely related to proofs by exhaustion we tried before.
- Sometimes when we want to prove a statement, there are many possible cases. Also, we might not know which cases are true.
- We might still be able to prove the statement if we can show that the statement is true in every case.

Example II (1)

Theorem

Suppose that I have 3 pairs of socks: one pair in gray, one pair in white, and one pair in black. If I pick any 4 socks, I will have at least one pair of the same color.

Example II (1)

Theorem

Suppose that I have 3 pairs of socks: one pair in gray, one pair in white, and one pair in black. If I pick any 4 socks, I will have at least one pair of the same color.

If we want to prove by exhaustion, we will have to consider all 15 cases.

Example II (1)

Theorem

Suppose that I have 3 pairs of socks: one pair in gray, one pair in white, and one pair in black. If I pick any 4 socks, I will have at least one pair of the same color.

If we want to prove by exhaustion, we will have to consider all 15 cases.

Proof.

Let's split the process of picking 4 socks into 2 steps. First, pick 3 socks, then pick the last sock.

After we pick the first 3 socks. There are 2 possible cases: either I have a pair of socks with the same color, or I do not have such a pair. We shall consider each case separately.

(cont. in the next slide) □

Example II (1)

Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*

Example II (1)

Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*
  In this case, the theorem is true.

Example II (1)

Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*
  In this case, the theorem is true.
- **Case 2:** *I do not have a pair of socks with the same color.*

Example II (1)

Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*
  In this case, the theorem is true.
- **Case 2:** *I do not have a pair of socks with the same color.*
  In this case, since I have 3 colors and 3 socks, I must have one sock for each color. Now, after we pick the last sock, whatever color the last one is, we have a color-matching sock in our first 3 socks. Therefore, the theorem is also true in this case.

Example II (1)

Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*
  In this case, the theorem is true.
- **Case 2:** *I do not have a pair of socks with the same color.*
  In this case, since I have 3 colors and 3 socks, I must have one sock for each color. Now, after we pick the last sock, whatever color the last one is, we have a color-matching sock in our first 3 socks. Therefore, the theorem is also true in this case.

Since these two cases cover all possibilities, we conclude that the theorem is true. □

Proofs by cases in propositional logic

In propositional logic, the following describe a proof by cases.

$$\begin{array}{l} \quad p \vee q \vee r \\ \quad p \rightarrow s \\ \quad q \rightarrow s \\ \quad r \rightarrow s \\ \hline \therefore s \end{array}$$

Proofs by cases in propositional logic

In propositional logic, the following describe a proof by cases.

$$\begin{array}{l} p \vee q \vee r \\ p \rightarrow s \\ q \rightarrow s \\ r \rightarrow s \\ \hline \therefore s \end{array}$$

Sometimes, when we have 2 cases, we also see:

Proofs by cases in propositional logic

In propositional logic, the following describe a proof by cases.

$$\begin{array}{l} p \vee q \vee r \\ p \rightarrow s \\ q \rightarrow s \\ r \rightarrow s \\ \hline \therefore s \end{array}$$

Sometimes, when we have 2 cases, we also see:

$$\begin{array}{l} p \vee \neg p \\ p \rightarrow s \\ \neg p \rightarrow s \\ \hline \therefore s \end{array}$$

Note that we can leave $p \vee \neg p$ out, because it is always true.

Mathematical Induction

- In this lecture, we will focus on how to prove properties on natural numbers.

Mathematical Induction

- In this lecture, we will focus on how to prove properties on natural numbers.
- For example, we may want to prove that for any integer $n \geq 1$,

$$\sum_{i=1}^{n} i = n(n+1)/2,$$

or for any integer $n \geq 1$,

$$\sum_{i=1}^{n} i^2 = \frac{n}{6}(n+1)(2n+1),$$

or for any integer $n \geq 4$, one can use only 2-baht coins and 3-baht coins to obtain exactly n baht.

A review of the summation notation (by examples)

- $\sum_{i=1}^{10} i = 1 + 2 + \cdots + 10.$
- $\sum_{i=7}^{9} (i^2 + i) = (7^2 + 7) + (8^2 + 8) + (9^2 + 9).$
- The range of the index may be sets. For example, let $A = \{1, 2, 4, 15\}$, we have that $\sum_{i \in A} i^2 = 1^2 + 2^2 + 4^2 + 15^2$.
- What is $\sum_{i=5}^{2} i$?

A review of the summation notation (by examples)

- $\displaystyle\sum_{i=1}^{10} i = 1 + 2 + \cdots + 10.$
- $\displaystyle\sum_{i=7}^{9} (i^2 + i) = (7^2 + 7) + (8^2 + 8) + (9^2 + 9).$
- The range of the index may be sets. For example, let $A = \{1, 2, 4, 15\}$, we have that $\displaystyle\sum_{i \in A} i^2 = 1^2 + 2^2 + 4^2 + 15^2.$
- What is $\sum_{i=5}^{2} i$?
  Note that in this case, the range is empty. This sum is called an **empty sum**. By convention, we define it to be zero.

Informal arguments (1)

- Let's try to check that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$, by experimentation.
- Try $n = 1$:

[1] LHS = left hand side

[2] RHS = right hand side

Informal arguments (1)

- Let's try to check that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$, by experimentation.
- Try $n = 1$: LHS[1]: 1,

[1]LHS = left hand side
[2]RHS = right hand side

Informal arguments (1)

- Let's try to check that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$, by experimentation.
- Try $n = 1$: LHS[1]: 1, RHS[2]: $1(1+1)/2 = 1$,

[1]LHS = left hand side
[2]RHS = right hand side

Informal arguments (1)

- Let's try to check that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$, by experimentation.
- Try $n = 1$: LHS[1]: 1, RHS[2]: $1(1+1)/2 = 1$, OK

[1] LHS = left hand side
[2] RHS = right hand side

Informal arguments (1)

- Let's try to check that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$, by experimentation.
- Try $n = 1$: LHS[1]: 1, RHS[2]: $1(1+1)/2 = 1$, OK
- Try $n = 2$: LHS: $1 + 2 = 3$, RHS: $2(2+1)/2 = 3$, OK

[1] LHS = left hand side
[2] RHS = right hand side

Informal arguments (1)

- Let's try to check that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$, by experimentation.
- Try $n = 1$: LHS[1]: 1, RHS[2]: $1(1+1)/2 = 1$, OK
- Try $n = 2$: LHS: $1 + 2 = 3$, RHS: $2(2+1)/2 = 3$, OK
- Try $n = 3$: LHS: $1 + 2 + 3 = 6$, RHS: $3(3+1)/2 = 6$, OK

[1] LHS = left hand side

[2] RHS = right hand side

Informal arguments (1)

- Let's try to check that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$, by experimentation.
- Try $n = 1$: LHS[1]: 1, RHS[2]: $1(1+1)/2 = 1$, OK
- Try $n = 2$: LHS: $1 + 2 = 3$, RHS: $2(2+1)/2 = 3$, OK
- Try $n = 3$: LHS: $1 + 2 + 3 = 6$, RHS: $3(3+1)/2 = 6$, OK
- Try ...

[1]LHS = left hand side
[2]RHS = right hand side

Informal arguments (1)

- Let's try to check that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$, by experimentation.
- Try $n = 1$: LHS[1]: 1, RHS[2]: $1(1+1)/2 = 1$, OK
- Try $n = 2$: LHS: $1 + 2 = 3$, RHS: $2(2+1)/2 = 3$, OK
- Try $n = 3$: LHS: $1 + 2 + 3 = 6$, RHS: $3(3+1)/2 = 6$, OK
- Try ...
- With this trying-all approach, we can't actually prove this statement.

[1] LHS = left hand side
[2] RHS = right hand side

Informal arguments (2)

- Our goal is to show that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$.
- Try $n = 2$: LHS: $1 + 2 = 3$, RHS: $2(2 + 1)/2 = 3$.
- Try $n = 3$: LHS: $1 + 2 + 3$, RHS: $3(3 + 1)/2$

Informal arguments (2)

- Our goal is to show that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$.
- Try $n = 2$: LHS: $1 + 2 = 3$, RHS: $2(2+1)/2 = 3$.
- Try $n = 3$: LHS: $1 + 2 + 3$, RHS: $3(3+1)/2$
- If we compare these two lines, we can see that

$$\begin{aligned}
1+2+3 &= (1+2)+3 \\
&= 2(2+1)/2+3 \qquad (*) \\
&= 2(2+1)/2+(2+1) \\
&= 2(2+1)/2+2\cdot(2+1)/2 \\
&= (2+2)(2+1)/2 = (3+1)(3)/2,
\end{aligned}$$

which is equal to $3(3+1)/2$.

Informal arguments (2)

- Our goal is to show that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$.
- Try $n = 2$: LHS: $1 + 2 = 3$, RHS: $2(2 + 1)/2 = 3$.
- Try $n = 3$: LHS: $1 + 2 + 3$, RHS: $3(3 + 1)/2$
- If we compare these two lines, we can see that

$$\begin{aligned} 1+2+3 &= (1+2)+3 \\ &= 2(2+1)/2+3 \qquad (*) \\ &= 2(2+1)/2+(2+1) \\ &= 2(2+1)/2+2\cdot(2+1)/2 \\ &= (2+2)(2+1)/2=(3+1)(3)/2, \end{aligned}$$

  which is equal to $3(3 + 1)/2$.
- Line (*) is important here. That is because we use the fact that the statement is true when $n = 2$ there.

Informal arguments (3)

- Goal: show that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$.
- What we have just done?

Informal arguments (3)

- Goal: show that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$.
- What we have just done? We show that the statement is true when $n = 3$ if it is true when $n = 2$.

Informal arguments (3)

- Goal: show that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$.
- What we have just done? We show that the statement is true when $n = 3$ if it is true when $n = 2$.
- Let's try to make a more general argument.

Informal arguments (3)

- Goal: show that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$.
- What we have just done? We show that the statement is true when $n = 3$ if it is true when $n = 2$.
- Let's try to make a more general argument.
- Assume that the statement is true for $n = k$. I.e.,

$$\sum_{i=1}^{k} i = k(k+1)/2.$$

Informal arguments (3)

- Goal: show that $\sum_{i=1}^{n} i = n(n+1)/2$, for any integer $n \geq 1$.
- What we have just done? We show that the statement is true when $n = 3$ if it is true when $n = 2$.
- Let's try to make a more general argument.
- Assume that the statement is true for $n = k$. I.e.,

$$\sum_{i=1}^{k} i = k(k+1)/2.$$

- Can we show that, with this assumption, the statement is true for $n = k+1$? I.e., can we show that

$$\sum_{i=1}^{k+1} i = (k+1)((k+1)+1)/2?$$

Informal arguments (4)

Let's try...

Assumption: $\sum_{i=1}^{k} i = k(k+1)/2$.

Goal: $\sum_{i=1}^{k+1} i = (k+1)((k+1)+1)/2$.

Informal arguments (4)

Let's try...
Assumption: $\sum_{i=1}^{k} i = k(k+1)/2$.
Goal: $\sum_{i=1}^{k+1} i = (k+1)((k+1)+1)/2$.

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1)$$

Informal arguments (4)

Let's try...

Assumption: $\sum_{i=1}^{k} i = k(k+1)/2$.

Goal: $\sum_{i=1}^{k+1} i = (k+1)((k+1)+1)/2$.

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= k(k+1)/2 + (k+1)
\end{aligned}$$

Informal arguments (4)

Let's try...

Assumption: $\sum_{i=1}^{k} i = k(k+1)/2$.

Goal: $\sum_{i=1}^{k+1} i = (k+1)((k+1)+1)/2$.

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1)\\ &= k(k+1)/2 + (k+1)\\ &= k(k+1)/2 + 2\cdot(k+1)/2\end{aligned}$$

Informal arguments (4)

Let's try...
Assumption: $\sum_{i=1}^{k} i = k(k+1)/2$.
Goal: $\sum_{i=1}^{k+1} i = (k+1)((k+1)+1)/2$.

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= k(k+1)/2 + (k+1) \\
&= k(k+1)/2 + 2 \cdot (k+1)/2 \\
&= (k+2)(k+1)/2 \\
&= (k+1)((k+1)+1)/2,
\end{aligned}$$

as required.

Informal arguments (5)

We have all the ingredients required to prove this statement:

For integer $n \geq 1$, $\sum_{i=1}^{n} i = n \cdot (n+1)/2$.

Informal arguments (5)

We have all the ingredients required to prove this statement:

> For integer $n \geq 1$, $\sum_{i=1}^{n} i = n \cdot (n+1)/2$.

Let $P(n) \equiv$ "$\sum_{i=1}^{n} i = n \cdot (n+1)/2$".
The statement we want to prove becomes:

> For any natural number n, $P(n)$.

Informal arguments (5)

We have all the ingredients required to prove this statement:

> For integer $n \geq 1$, $\sum_{i=1}^{n} i = n \cdot (n+1)/2$.

Let $P(n) \equiv$ "$\sum_{i=1}^{n} i = n \cdot (n+1)/2$".
The statement we want to prove becomes:

> For any natural number n, $P(n)$.

We have shown:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

Informal arguments (6)

We have:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

$P(1)$ (1st statement itself)

Informal arguments (6)

We have:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

$P(1)$ (1st statement itself)
$\Rightarrow P(2)$ (from 2nd statement, let $k = 1$)

Informal arguments (6)

We have:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

$P(1)$ (1st statement itself)
$\Rightarrow P(2)$ (from 2nd statement, let $k = 1$)
$\Rightarrow P(3)$ (from 2nd statement, let $k = 2$)

Informal arguments (6)

We have:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

$P(1)$ (1st statement itself)
$\Rightarrow P(2)$ (from 2nd statement, let $k = 1$)
$\Rightarrow P(3)$ (from 2nd statement, let $k = 2$)
$\Rightarrow P(4)$ (from 2nd statement, let $k = 3$)

Informal arguments (6)

We have:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

$P(1)$ (1st statement itself)
$\Rightarrow P(2)$ (from 2nd statement, let $k = 1$)
$\Rightarrow P(3)$ (from 2nd statement, let $k = 2$)
$\Rightarrow P(4)$ (from 2nd statement, let $k = 3$)
$\Rightarrow P(5)$

Informal arguments (6)

We have:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

$P(1)$ (1st statement itself)
$\Rightarrow P(2)$ (from 2nd statement, let $k = 1$)
$\Rightarrow P(3)$ (from 2nd statement, let $k = 2$)
$\Rightarrow P(4)$ (from 2nd statement, let $k = 3$)
$\Rightarrow P(5) \Rightarrow P(6)$

Informal arguments (6)

We have:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

$P(1)$ (1st statement itself)
$\Rightarrow P(2)$ (from 2nd statement, let $k = 1$)
$\Rightarrow P(3)$ (from 2nd statement, let $k = 2$)
$\Rightarrow P(4)$ (from 2nd statement, let $k = 3$)
$\Rightarrow P(5) \Rightarrow P(6) \Rightarrow P(7)$

Informal arguments (6)

We have:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

$P(1)$ (1st statement itself)
$\Rightarrow P(2)$ (from 2nd statement, let $k = 1$)
$\Rightarrow P(3)$ (from 2nd statement, let $k = 2$)
$\Rightarrow P(4)$ (from 2nd statement, let $k = 3$)
$\Rightarrow P(5) \Rightarrow P(6) \Rightarrow P(7) \ldots$

Informal arguments (6)

We have:

1. $P(1)$ (by experimentation)
2. $P(k) \Rightarrow P(k+1)$ for any integer $k \geq 1$.

What do these two statements imply?

$P(1)$ (1st statement itself)
$\Rightarrow P(2)$ (from 2nd statement, let $k = 1$)
$\Rightarrow P(3)$ (from 2nd statement, let $k = 2$)
$\Rightarrow P(4)$ (from 2nd statement, let $k = 3$)
$\Rightarrow P(5) \Rightarrow P(6) \Rightarrow P(7) \ldots$

Informally, these chain of reasoning will eventually reach any natural number n. Therefore, we can conclude that $P(n)$ for any natural number n.

We have just shown the statement with mathematical induction.

Mathematical induction

Suppose that you want to prove that property $P(n)$ is true for every natural number n.

Suppose that we can prove the following two facts:
Base case: $P(1)$
Inductive step: For any $k \geq 1$, $P(k) \Rightarrow P(k+1)$

The **Principle of Mathematical Induction** states that $P(n)$ is true for every natural number n.

The assumption $P(k)$ in the inductive step is usually referred to as **the Induction Hypothesis**.

Let's re-write the proof again

Theorem

For every natural number n, $\sum_{i=1}^{n} i = n(n+1)/2$

Proof: We prove by induction. The property that we want to prove $P(n)$ is "$\sum_{i=1}^{n} i = n(n+1)/2$."

Base case: We can plug in $n = 1$ to check that $P(1)$ is true: $1 = 1(1+1)/2$.

Inductive step: We assume that $P(k)$ is true for $k \geq 1$ and show that $P(k+1)$ is true.

Let's state the Induction Hypothesis $P(k)$: $\sum_{i=1}^{k} i = k(k+1)/2$.

Let's show $P(k+1)$. We write $\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1)$. Using the Induction Hypothesis, we know that this is equal to

$$\begin{aligned} k(k+1)/2 + (k+1) &= k(k+1)/2 + 2 \cdot (k+1) \\ &= (k+2)(k+1)/2, \end{aligned}$$

which implies $P(k+1)$ as required.

From the Principle of Mathematical Induction, this implies that $P(n)$ is true for every natural number n.

Review: mathematical induction

Suppose that you want to prove that property $P(n)$ is true for every natural number n.

Suppose that we can prove the following two facts:
Base case: $P(1)$
Inductive step: For any $k \geq 1$, $P(k) \Rightarrow P(k+1)$

The **Principle of Mathematical Induction** states that $P(n)$ is true for every natural number n.

The assumption $P(k)$ in the inductive step is usually referred to as **the Induction Hypothesis**.

Example III

Theorem: For every natural number n, $\sum_{i=1}^{n} i^2 = \frac{n}{6}(n+1)(2n+1)$

Proof: We prove by induction. The property that we want to prove $P(n)$ is "$\sum_{i=1}^{n} i^2 = \frac{n}{6}(n+1)(2n+1)$."

Base case: We can plug in $n = 1$ to check that $P(1)$ is true: $1^2 = \frac{1}{6}(1+1)(2 \cdot 1 + 1)$.

Inductive step: We assume that $P(k)$ is true for $k \geq 1$ and show that $P(k+1)$ is true.

We first assume the Induction Hypothesis $P(k)$: $\sum_{i=1}^{k} i^2 = \frac{k}{6}(k+1)(2k+1)$

(continue on the next page)

Example III (cont.)

Let's show $P(k+1)$. We write $\sum_{i=1}^{k+1} i^2 = \left(\sum_{i=1}^{k} i^2\right) + (k+1)^2$.

Using the Induction Hypothesis, we know that this is equal to

$$\begin{aligned}(k/6)(k+1)(2k+1)+(k+1)^2 &= \frac{(k+1)}{6}(k(2k+1)+6(k+1)) \\ &\quad \text{(In this step, we factor out } (k+1)/6\text{)} \\ &= \frac{(k+1)}{6}(2k^2+7k+6) \\ &= \frac{(k+1)}{6}((k+1)+1)(2(k+1)+1).\end{aligned}$$

This implies $P(k+1)$ as required.
From the Principle of Mathematical Induction, this implies that $P(n)$ is true for every natural number n. ■

Unused facts

- Let's informally think about how proving $P(1)$ and $P(k) \Rightarrow P(k+1)$ for all $k \geq 1$ implies that $P(n)$ is true for all natural number n.

Unused facts

- Let's informally think about how proving $P(1)$ and $P(k) \Rightarrow P(k+1)$ for all $k \geq 1$ implies that $P(n)$ is true for all natural number n.
- One may notice that when we prove a statement $P(n)$ for all natural number n by induction, during the inductive step where we want to show $P(k+1)$ from $P(k)$, we usually have that $P(1), P(2), \ldots, P(k)$ is true at hands as well.
- Then why don't we use them as well?

Strong mathematical induction

Strong induction

Suppose that you want to prove that property $P(n)$ is true for every natural number n.

Suppose that we can prove the following two facts:

Strong mathematical induction

Strong induction

Suppose that you want to prove that property $P(n)$ is true for every natural number n.

Suppose that we can prove the following two facts: **Base case:** $P(1)$

Inductive step: For any $k \geq 1$,

$$P(1) \wedge P(2) \wedge \cdots \wedge P(k) \Rightarrow P(k+1).$$

Then $P(n)$ is true for every natural number n.

Example IV

Theorem: For any integer $n \geq 4$, one can use only 2-baht coins and 3-baht coins to obtain exactly n baht.

Proof: We prove by strong induction on n.

Example IV

Theorem: For any integer $n \geq 4$, one can use only 2-baht coins and 3-baht coins to obtain exactly n baht.

Proof: We prove by strong induction on n.
Base cases: For $n = 4$, we can use two 2-baht coins. For $n = 5$, we can use one 2-baht coin and one 3-baht coin.

Example IV

Theorem: For any integer $n \geq 4$, one can use only 2-baht coins and 3-baht coins to obtain exactly n baht.

Proof: We prove by strong induction on n.
Base cases: For $n = 4$, we can use two 2-baht coins. For $n = 5$, we can use one 2-baht coin and one 3-baht coin.

Inductive step: Assume that for $k \geq 5$, we can obtain exactly ℓ baht, for $4 \leq \ell \leq k$, using only 2-baht and 3-baht coins. We will show how to obtain a set of $k + 1$ baht.

Example IV

Theorem: For any integer $n \geq 4$, one can use only 2-baht coins and 3-baht coins to obtain exactly n baht.

Proof: We prove by strong induction on n.
Base cases: For $n = 4$, we can use two 2-baht coins. For $n = 5$, we can use one 2-baht coin and one 3-baht coin.

Inductive step: Assume that for $k \geq 5$, we can obtain exactly ℓ baht, for $4 \leq \ell \leq k$, using only 2-baht and 3-baht coins. We will show how to obtain a set of $k + 1$ baht.
Since $k \geq 5$, we have that $k - 1 \geq 4$. Therefore from the Induction Hypothesis, we can use only 2-baht coins and 3-baht coins to form a set of coins of total value $k - 1$ baht.

Example IV

Theorem: For any integer $n \geq 4$, one can use only 2-baht coins and 3-baht coins to obtain exactly n baht.

Proof: We prove by strong induction on n.
Base cases: For $n = 4$, we can use two 2-baht coins. For $n = 5$, we can use one 2-baht coin and one 3-baht coin.

Inductive step: Assume that for $k \geq 5$, we can obtain exactly ℓ baht, for $4 \leq \ell \leq k$, using only 2-baht and 3-baht coins. We will show how to obtain a set of $k + 1$ baht.
Since $k \geq 5$, we have that $k - 1 \geq 4$. Therefore from the Induction Hypothesis, we can use only 2-baht coins and 3-baht coins to form a set of coins of total value $k - 1$ baht. With one additional 2-baht coin, we can obtain a set of value $(k - 1) + 2 = k + 1$ baht, as required.

Example IV

Theorem: For any integer $n \geq 4$, one can use only 2-baht coins and 3-baht coins to obtain exactly n baht.

Proof: We prove by strong induction on n.
Base cases: For $n = 4$, we can use two 2-baht coins. For $n = 5$, we can use one 2-baht coin and one 3-baht coin.

Inductive step: Assume that for $k \geq 5$, we can obtain exactly ℓ baht, for $4 \leq \ell \leq k$, using only 2-baht and 3-baht coins. We will show how to obtain a set of $k + 1$ baht.
Since $k \geq 5$, we have that $k - 1 \geq 4$. Therefore from the Induction Hypothesis, we can use only 2-baht coins and 3-baht coins to form a set of coins of total value $k - 1$ baht. With one additional 2-baht coin, we can obtain a set of value $(k - 1) + 2 = k + 1$ baht, as required.

From the Principle of Strong Mathematical Induction, we conclude that the theorem is true. ■

Is strong induction more powerful?

- Can we prove the previous theorem without using the strong induction?

Is strong induction more powerful?

- Can we prove the previous theorem without using the strong induction? Yes, you can (homework).

Is strong induction more powerful?

- Can we prove the previous theorem without using the strong induction? Yes, you can (homework).
- In fact, if you can prove that $P(n)$ is true for all natural number n with strong induction. You can always prove it with mathematical induction.

Is strong induction more powerful?

- Can we prove the previous theorem without using the strong induction? Yes, you can (homework).
- In fact, if you can prove that $P(n)$ is true for all natural number n with strong induction. You can always prove it with mathematical induction.
- Hint: Let $Q(n) = P(1) \land P(2) \land \cdots \land P(n)$.

Review: mathematical induction

Suppose that you want to prove that property $P(n)$ is true for every natural number n.

Suppose that we can prove the following two facts:
Base case: $P(1)$
Inductive step: For any $k \geq 1$, $P(k) \Rightarrow P(k+1)$

The **Principle of Mathematical Induction** states that $P(n)$ is true for every natural number n.

The assumption $P(k)$ in the inductive step is usually referred to as **the Induction Hypothesis**.

The induction hypothesis

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$.

The induction hypothesis

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$.

Proof.

The statement $P(n)$ that we want to prove is
"$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$".

The induction hypothesis

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$.

Proof.

The statement $P(n)$ that we want to prove is "$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$".

Case case: For $n = 1$, the statement is true because $1 < 2$.

The induction hypothesis

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$.

Proof.

The statement $P(n)$ that we want to prove is "$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$".

Case case: For $n = 1$, the statement is true because $1 < 2$.

Inductive step: For $k \geq 1$, let's assume $P(k)$ and we prove that $P(k+1)$ is true.

The induction hypothesis

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$.

Proof.

The statement $P(n)$ that we want to prove is "$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$".

Case case: For $n = 1$, the statement is true because $1 < 2$.

Inductive step: For $k \geq 1$, let's assume $P(k)$ and we prove that $P(k+1)$ is true.

The induction hypothesis is: $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{k^2} < 2$.

We want to show $P(k+1)$, i.e., $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} < 2$.

Then... □

Strengtening the Induction Hypothesis (1)

- Is the assumption

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{k^2} < 2.$$

"strong" enough to prove

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} < 2 \quad ?$$

Why?

Strengtening the Induction Hypothesis (1)

- Is the assumption

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{k^2}<2.$$

"strong" enough to prove

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{k^2}+\frac{1}{(k+1)^2}<2 \quad ?$$

Why?

- To prove $P(k+1)$, we need a "gap" between the LHS and 2, so that we can add $1/(k+1)^2$ without blowing up the RHS.

Strengtening the Induction Hypothesis (2)

- Let's see a few values of the sum:
  - $1/1 = 1$.
  - $1/1 + 1/4 = 1.25$.
  - $1/1 + 1/4 + 1/9 \approx 1.361$.
  - $1/1 + 1/4 + 1/9 + 1/16 \approx 1.4236$.
  - $1/1 + 1/4 + 1/9 + 1/16 + 1/25 \approx 1.4636$.

  Yes, there is a gap. But how large?

Strengtening the Induction Hypothesis (2)

- Let's see a few values of the sum:
  - $1/1 = 1$.
  - $1/1 + 1/4 = 1.25$.
  - $1/1 + 1/4 + 1/9 \approx 1.361$.
  - $1/1 + 1/4 + 1/9 + 1/16 \approx 1.4236$.
  - $1/1 + 1/4 + 1/9 + 1/16 + 1/25 \approx 1.4636$.

  Yes, there is a gap. But how large?
- We need the gap to be large enough to insert $1/(k+1)^2$.

Strengtening the Induction Hypothesis (2)

- Let's see a few values of the sum:
  - $1/1 = 1$.
  - $1/1 + 1/4 = 1.25$.
  - $1/1 + 1/4 + 1/9 \approx 1.361$.
  - $1/1 + 1/4 + 1/9 + 1/16 \approx 1.4236$.
  - $1/1 + 1/4 + 1/9 + 1/16 + 1/25 \approx 1.4636$.

  Yes, there is a gap. But how large?
- We need the gap to be large enough to insert $1/(k+1)^2$.
- After a "mysterious" moment, we observe that

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

Strengtening the Induction Hypothesis (3)

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$.

Strengtening the Induction Hypothesis (3)

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$.

Proof.

(... the beginning is left out ...)
Inductive step: For $k \geq 1$, assume that $\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} \leq 2 - \frac{1}{k}$.

Strengtening the Induction Hypothesis (3)

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$.

Proof.

(... the beginning is left out ...)
Inductive step: For $k \geq 1$, assume that $\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} \leq 2 - \frac{1}{k}$.
Adding $1/(k+1)^2$ on both sides, we get

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{k} + \frac{1}{(k+1)^2} = 2 - \left(\frac{1}{k} - \frac{1}{(k+1)^2}\right).$$

Strengtening the Induction Hypothesis (3)

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$.

Proof.

(... the beginning is left out ...)

Inductive step: For $k \geq 1$, assume that $\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} \leq 2 - \frac{1}{k}$.

Adding $1/(k+1)^2$ on both sides, we get

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{k} + \frac{1}{(k+1)^2} = 2 - \left(\frac{1}{k} - \frac{1}{(k+1)^2}\right).$$

Since $1/k - 1/(k+1) = 1/(k(k+1))$, we have that

$$1/(k+1) = 1/k - 1/(k(k+1)) < 1/k - 1/(k+1)^2.$$

Strengtening the Induction Hypothesis (3)

Theorem

For any integer $n \geq 1$, $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$.

Proof.

(... the beginning is left out ...)
Inductive step: For $k \geq 1$, assume that $\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} \leq 2 - \frac{1}{k}$.
Adding $1/(k+1)^2$ on both sides, we get

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{k} + \frac{1}{(k+1)^2} = 2 - \left(\frac{1}{k} - \frac{1}{(k+1)^2}\right).$$

Since $1/k - 1/(k+1) = 1/(k(k+1))$, we have that

$$1/(k+1) = 1/k - 1/(k(k+1)) < 1/k - 1/(k+1)^2.$$

Therefore, we conclude that

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \leq 2 - \left(\frac{1}{k} - \frac{1}{(k+1)^2}\right) \leq 2 - \frac{1}{k+1},$$

A Lesson learned

- Is a stronger statement easier to prove?

A Lesson learned

- Is a stronger statement easier to prove?
- In this case, the statement is indeed stronger, but the induction hypothesis gets stronger as well. Sometimes, this works out nicely.

Proof of the principle of mathematical induction[3]

Theorem

If $P(1)$ and for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, then $P(n)$ for all natural number n.

Proof.

[3] This section is from Berkeley CS70 lecture notes.

Proof of the principle of mathematical induction[3]

Theorem

If $P(1)$ and for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, then $P(n)$ for all natural number n.

Proof.

We prove by contradiction.

[3] This section is from Berkeley CS70 lecture notes.

Proof of the principle of mathematical induction[3]

Theorem

If $P(1)$ and for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, then $P(n)$ for all natural number n.

Proof.

We prove by contradiction. Assume that $P(n)$ is not true for some natural number n.

[3] This section is from Berkeley CS70 lecture notes.

Proof of the principle of mathematical induction[3]

Theorem

If $P(1)$ and for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, then $P(n)$ for all natural number n.

Proof.

We prove by contradiction. Assume that $P(n)$ is not true for some natural number n. Let m be the smallest positive integer such that $P(m)$ is false.

[3] This section is from Berkeley CS70 lecture notes.

Proof of the principle of mathematical induction[3]

Theorem

If $P(1)$ and for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, then $P(n)$ for all natural number n.

Proof.

We prove by contradiction. Assume that $P(n)$ is not true for some natural number n. Let m be the smallest positive integer such that $P(m)$ is false. If $m = 1$, we get a contradiction because we know that $P(1)$ is true; therefore, we know that $m > 1$.

[3] This section is from Berkeley CS70 lecture notes.

Proof of the principle of mathematical induction[3]

Theorem

If $P(1)$ and for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, then $P(n)$ for all natural number n.

Proof.

We prove by contradiction. Assume that $P(n)$ is not true for some natural number n. Let m be the smallest positive integer such that $P(m)$ is false. If $m = 1$, we get a contradiction because we know that $P(1)$ is true; therefore, we know that $m > 1$.

Since m is smallest and $m > 1$, then $P(m-1)$ must be true.

[3] This section is from Berkeley CS70 lecture notes.

Proof of the principle of mathematical induction[3]

Theorem

If $P(1)$ and for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, then $P(n)$ for all natural number n.

Proof.

We prove by contradiction. Assume that $P(n)$ is not true for some natural number n. Let m be the smallest positive integer such that $P(m)$ is false. If $m = 1$, we get a contradiction because we know that $P(1)$ is true; therefore, we know that $m > 1$.
Since m is smallest and $m > 1$, then $P(m-1)$ must be true. However, because for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, we can conclude that $P(m)$ must be true. Again, we reach a contradiction.

[3] This section is from Berkeley CS70 lecture notes.

Proof of the principle of mathematical induction[3]

Theorem

If $P(1)$ and for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, then $P(n)$ for all natural number n.

Proof.

We prove by contradiction. Assume that $P(n)$ is not true for some natural number n. Let m be the smallest positive integer such that $P(m)$ is false. If $m = 1$, we get a contradiction because we know that $P(1)$ is true; therefore, we know that $m > 1$.

Since m is smallest and $m > 1$, then $P(m-1)$ must be true. However, because for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, we can conclude that $P(m)$ must be true. Again, we reach a contradiction.

Therefore, $P(n)$ is true for every positive integer n. □

[3] This section is from Berkeley CS70 lecture notes.

Proof of the principle of mathematical induction[3]

Theorem

If $P(1)$ and for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, then $P(n)$ for all natural number n.

Proof.

We prove by contradiction. Assume that $P(n)$ is not true for some natural number n. Let m be the smallest positive integer such that $P(m)$ is false. If $m = 1$, we get a contradiction because we know that $P(1)$ is true; therefore, we know that $m > 1$.

Since m is smallest and $m > 1$, then $P(m-1)$ must be true. However, because for any integer $k \geq 1$, $P(k) \Rightarrow P(k+1)$, we can conclude that $P(m)$ must be true. Again, we reach a contradiction.

Therefore, $P(n)$ is true for every positive integer n. □

Is this proof correct?

[3] This section is from Berkeley CS70 lecture notes.

The well-ordering property

- The proof of the Principle of Mathematical Induction depends on the following axiom of natural numbers $\mathbb{N}$:

The Well-Ordering Property: Any nonempty subset $S \subseteq \mathbb{N}$ contains the smallest element.

The well-ordering property

- The proof of the Principle of Mathematical Induction depends on the following axiom of natural numbers $\mathbb{N}$:

> **The Well-Ordering Property:** Any nonempty subset $S \subseteq \mathbb{N}$ contains the smallest element.

- Previously, we use the well-ordering property of natural numbers to prove the Principle of Mathematical Induction, but it turns out that we can use the induction to prove the well-ordering property as well.

The well-ordering property

- The proof of the Principle of Mathematical Induction depends on the following axiom of natural numbers $\mathbb{N}$:

> **The Well-Ordering Property:** Any nonempty subset $S \subseteq \mathbb{N}$ contains the smallest element.

- Previously, we use the well-ordering property of natural numbers to prove the Principle of Mathematical Induction, but it turns out that we can use the induction to prove the well-ordering property as well. Therefore, we can take one as an axiom, and use it to prove the other.

Take-aways

Conclusion

- Rules of inferences
- Introduction to proofs
- Proof methods and strategies
    - Direct proofs
    - Proofs by contraposition
    - Proofs by contradiction
    - Proofs by cases
    - Mathematical induction