Discrete Mathematics for Computer Science

Lecture 3: Nested Quantifier, Mathematical Proofs

Dr. Ming Tang

Department of Computer Science and Engineering
Southern University of Science and Technology (SUSTech)
Email: tangm3@sustech.edu.cn

Questions from Students: Limitations of Proposition

- p: Every computer in Room 101 is functioning properly.
- q: Computer MATH3 is in Room 101.

Can we conclude r: "MATH3 is functioning properly" using the rules of propositional logic? NO! Cannot infer r from p and q.

With predicate and quantifier:

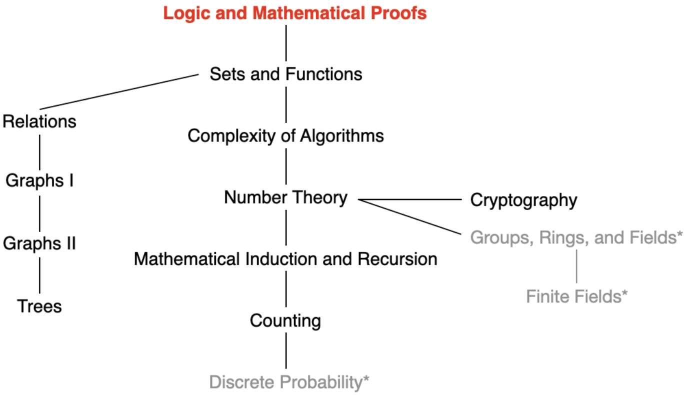
- $C(x)$: Computer x is in Room 101.
- $D(x)$: Computer x is functioning properly.

- $\forall x(C(x) \rightarrow D(x))$ within the domain of computers: Every computer in Room 101 is functioning properly.
- $C(MATH3)$: Computer MATH3 is in Room 101.
- $D(MATH3)$: MATH3 is functioning properly.

Review: Predicates and Quantifier

- Predicate:
  - Propositional function $P(x)$
  - domain of variable x
  - If x is specified, $P(x)$ becomes a Proposition
- Quantifier
  - Universal quantifier $\forall x P(x)$
  - Existential quantifier $\exists x P(x)$
  - $\forall x P(x)$ and $\exists x P(x)$ are propositions

This Lecture



Logic: Propositional logic, applications of propositional logic, propositional equivalence, predicates and quantifiers, nested quantifiers
Mathematical Proofs: Rules of inference, introduction to proofs,

Nested Quantifiers

More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

Example 1: For every real number, there is another real number such that their summation is equal to zero.

- $P(x, y)$: $x + y = 0$
- Domain of x and y: all real number
- $\forall x \exists y P(x, y)$

Nested Quantifiers

More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

Example 2: There is a real number such that it is larger than all negative real numbers.

- $P(x, y)$: $x > y$
- Domain of x: all real number
- Domain of y: all negative real numbers
- $\exists x \forall y P(x, y)$

Does the order matter?

Order of Quantifiers

The order of nested quantifiers matters if quantifiers are of different type.

Example:

- $P(x, y)$: $x + y = 0$
- Domain of x: all real number
- Domain of y: all negative real numbers

$\forall x \exists y P(x, y)$ is not equivalent to $\exists y \forall x P(x, y)$

- $\forall x \exists y P(x, y)$: for every x, there exists a y such that ...
- $\exists y \forall x P(x, y)$: exists a y such that for every x ...

Note: for the simplicity of understanding, read $\forall x P(x)$ as "for every x, $P(x)$ ...."

Order of Quantifiers

The order of nested quantifiers does no matter if quantifiers are of the same type.

Example:

- $P(x, y)$: $x + y = y + x$
- Domain of x: all real number
- Domain of y: all negative real numbers

$\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y)$:

- $\exists x \exists y P(x, y)$: exists an x such that there exists a y ...
- $\exists y \exists x P(x, y)$: exists a y such that there exists an x ...

$\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$:

Order of Quantifiers

The order of nested quantifiers does no matter if quantifiers are of the same type.

Example:

- $P(x, y)$: $x + y = y + x$
- Domain of x: all real number
- Domain of y: all negative real numbers

$\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y)$: Exist a pair x, y for which $P(x, y)$ is true.

$\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$:

- $\forall x \forall y P(x, y)$: for every x, for every y, ...
- $\forall y \forall x P(x, y)$: for every y, for every x, ...

Order of Quantifiers

The order of nested quantifiers does no matter if quantifiers are of the same type.

Example:

- $P(x, y)$: $x + y = y + x$
- Domain of x: all real number
- Domain of y: all negative real numbers

$\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y)$: Exist a pair x, y for which $P(x, y)$ is true.

$\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$: For every pair x, y, $P(x, y)$ is true.

Nest Quantifier with Two Variables

Statement	*When True?*	*When False?*
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y.	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y.	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y.

Try to Translate

1. The sum of two positive integers is always positive.
   - Domain of x and y: all integers
   - $P(x, y)$: $(x > 0) \wedge (y > 0)$
   - $Q(x, y)$: $x + y > 0$
   - $\forall x \forall y (P(x, y) \rightarrow Q(x, y))$
   - Or, we can write it as $\forall x \forall y ((x > 0) \wedge (y > 0) \rightarrow x + y > 0)$
2. Every real number except zero has a multiplicative inverse.
   - Domain of x and y: all real numbers
   - $\forall x ((x \neq 0) \rightarrow \exists y (xy = 1))$

Inverse:
xy=1

A Question from Students

Are $\forall x((x \neq 0) \rightarrow \exists y(xy = 1))$ and $\forall x \exists y((x \neq 0) \rightarrow (xy = 1))$ equivalent?

Quick Answer: Yes. This is because $p \rightarrow \exists y Q(y)$ and $\exists y(p \rightarrow Q(y))$ are equivalent. To prove this, see page 45 in the textbook:

- If $p \rightarrow \exists y Q(y)$ is true, then $\exists y(p \rightarrow Q(y))$ is true;
- If $\exists y(p \rightarrow Q(y))$ is true, then $p \rightarrow \exists y Q(y)$ is true.

Complicated Answer: (out of the scope of this course)

- Free variable: $\sum_{k=1}^{10} f(k, n)$, n is a free variable

Where φ is any formula and where x is not a free variable in ψ:

$\forall x\, \varphi \rightarrow \psi \Leftrightarrow \forall x(\varphi \rightarrow \psi)$ (No!)

$\psi \rightarrow \forall x\, \varphi \Leftrightarrow \forall x(\psi \rightarrow \varphi)$ (Yes!)

$\exists x\, \varphi \rightarrow \psi \Leftrightarrow \exists x(\varphi \rightarrow \psi)$ (No!)

$\psi \rightarrow \exists x\, \varphi \Leftrightarrow \exists x(\psi \rightarrow \varphi)$ (Yes!)

SUSTech

Negating Nested Quantifiers

For every real number x, there exists a real number y such that $xy = 1$.

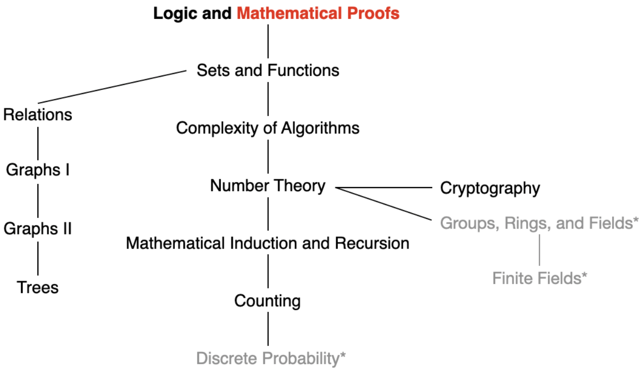
$$\forall x \exists y (xy = 1)$$

$$\begin{aligned} & \neg \forall x \exists y \ (xy = 1) \\ \equiv \ & \exists x \neg \exists y \ (xy = 1) \\ \equiv \ & \exists x \forall y \ \neg (xy = 1) \\ \equiv \ & \exists x \forall y \ (xy \neq 1) \end{aligned}$$

Note: $\neg(\forall x P(x)) \equiv \exists x(\neg P(x))$, $\neg(\exists x P(x)) \equiv \forall x(\neg P(x))$

SUSTech Southern University of Science and Technology

This Lecture



Mathematical Proofs: Rules of inference, introduction to proofs

Argument

Argument: A sequence of propositions that end with a conclusion.

"If you have a current password, then you can log onto the network."

"You have a current password."

Therefore,

"You can log onto the network."

Arguments consist of premises and conclusions

Argument: A sequence of propositions that end with a conclusion.

Premises:

"If you have a current password, then you can log onto the network."

"You have a current password."

Conclusion:

"You can log onto the network."

An argument is valid if the truth of all its premises implies that the conclusion is true.

Argument Form

Premises:

"If you have a current password, then you can log onto the network."

"You have a current password."

Conclusion: "You can log onto the network."

An argument form in propositional logic is a sequence of compound propositions involving propositional variables.

- p: "You have a current password"
- q: "You can log onto the network" or "You can change your grade"

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

The validity of an argument follows from the validity of its argument form.

Validity

Validity of Argument Form: The argument form with premises $p_1, p_2, ..., p_n$ and conclusion q is valid, if

$$(p_1 \land p_2 \land \cdots \land p_n) \to q \text{ is a tautology.}$$

Validity

Validity of Argument Form: The argument form with premises $p_1, p_2, ..., p_n$ and conclusion q is valid, if

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q \text{ is a tautology.}$$

Note: According to the definition of $p \rightarrow q$, we do not worry about the case where $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ is false.

Thus, equivalently, an argument form is valid no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

Validity

Validity of Argument Form: The argument form with premises $p_1, p_2, ..., p_n$ and conclusion q is valid, if

$$(p_1 \land p_2 \land \cdots \land p_n) \to q \text{ is a tautology.}$$

Is the following argument form valid?

$$\begin{array}{rl} & p \to q \\ & p \\ \hline \therefore & q \end{array}$$

Validity

Validity of Argument Form: The argument form with premises $p_1, p_2, ..., p_n$ and conclusion q is valid, if

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q \text{ is a tautology.}$$

Is the following argument form valid?

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

Is $(p \rightarrow q) \wedge p \rightarrow q$ a tautology?

Validity

Validity of Argument Form: The argument form with premises $p_1, p_2, ..., p_n$ and conclusion q is valid, if

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q \text{ is a tautology.}$$

Validity of Argument: The validity of an argument follows from the validity of the form of the argument.

Validity

Validity of Argument Form: The argument form with premises $p_1, p_2, ..., p_n$ and conclusion q is valid, if

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q \text{ is a tautology.}$$

Validity of Argument: The validity of an argument follows from the validity of the form of the argument.

Is the following argument valid?

"If you have access to the network, then you can change your grade."
"You have access to the network."

$\therefore$ "You can change your grade."

Validity

Validity of Argument Form: The argument form with premises $p_1, p_2, ..., p_n$ and conclusion q is valid, if

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q \text{ is a tautology.}$$

Validity of Argument: The validity of an argument follows from the validity of the form of the argument.

Is the following argument valid? Yes, because the argument form is valid.

"If you have access to the network, then you can change your grade."
"You have access to the network."

$\therefore$ "You can change your grade."

Validity

Is the following argument valid?

- If you do every problem in this book, then you will learn discrete mathematics.
- You learned discrete mathematics.
- Therefore, you did every problem in this book.

$$p \to q$$
$$\neg q$$
$$\overline{\qquad\qquad}$$
$$\therefore \neg p$$

Validity

Is the following argument valid?

- If you do every problem in this book, then you will learn discrete mathematics.
- You learned discrete mathematics.
- Therefore, you did every problem in this book.

No! $((p \rightarrow q) \land q) \rightarrow p$ is not a tautology.

Validity

Is the following argument valid?

- If you do every problem in this book, then you will learn discrete mathematics.
- You did not do every problem in this book.
- Therefore, you did not learn discrete mathematics.

Validity

Is the following argument valid?

- If you do every problem in this book, then you will learn discrete mathematics.
- You did not do every problem in this book.
- Therefore, you did not learn discrete mathematics.

No! $((p \to q) \land \neg p) \to \neg p$ is not a tautology.

Rules of Inference for Propositional Logic

To see the validity of $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$, we need to draw a table with 2^{n+1} row.

Rules of Inference for Propositional Logic

To see the validity of $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$, we need to draw a table with 2^{n+1} row. A tedious approach!

Construct complicated valid argument forms using the validity of some relatively simple argument forms, called rules of inference.

Rules of Inference for Propositional Logic

To see the validity of $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$, we need to draw a table with 2^{n+1} row.

Construct complicated valid argument forms using the validity of some relatively simple argument forms, called rules of inference.

- **modus ponens** (*law of detachment*) 肯定前件式

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

corresponding tautology:
$(p \wedge (p \rightarrow q)) \rightarrow q$

Rules of Inference for Propositional Logic

- **modus tollens** 否定后件式

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

corresponding tautology:
$(\neg q \land (p \to q)) \to \neg p$

- **hypothetical syllogism** 假言三段论

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

corresponding tautology:
$((p \to q) \land (q \to r)) \to (p \to r)$

Rules of Inference for Propositional Logic

- **disjunctive syllogism** 选言三段论

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

corresponding tautology:
$(\neg p \land (p \lor q)) \to q$

- **Addition**

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

corresponding tautology:
$p \to (p \lor q)$

- **Simplication**

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

corresponding tautology:
$(p \land q) \to p$

Rules of Inference for Propositional Logic

- **Conjunction**

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

corresponding tautology:
$((p) \wedge (q)) \rightarrow (p \wedge q)$

- **Resolution**

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

corresponding tautology:
$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$

Example

Show that the premises (i) $(p \wedge q) \vee r$ and (ii) $r \rightarrow s$ imply the conclusion $p \vee s$.

1.	$(p \vee r) \wedge (q \vee r)$	Premise (i), Distributive Law
2.	$p \vee r$	Simplification from step 1
3.	$\neg r \vee s$	Premise (ii), Useful Law
4.	$p \vee s$	Resolution

Using Rules of Inference to Build Arguments

- "It is not sunny this afternoon and it is colder than yesterday."
- "We will go swimming only if it is sunny."
- "If we do not go swimming then we will take a canoe trip."
- "If we take a canoe trip, then we will be home by sunset."
- Show the conclusion that "we will be home by sunset."

Using Rules of Inference to Build Arguments

- "It is not sunny this afternoon and it is colder than yesterday."
- "We will go swimming only if it is sunny."
- "If we do not go swimming then we will take a canoe trip."
- "If we take a canoe trip, then we will be home by sunset."
- Show the conclusion that "we will be home by sunset."

- p: It is sunny this afternoon.
- q: It is colder than yesterday.
- r: We will go swimming.
- s: We will take a canoe trip.
- t: We will be home by sunset.

Using Rules of Inference to Build Arguments

- "It is not sunny this afternoon and it is colder than yesterday."

  $\neg p \land q$
- "We will go swimming only if it is sunny."

  $r \rightarrow p$
- "If we do not go swimming then we will take a canoe trip."

  $\neg r \rightarrow s$
- "If we take a canoe trip, then we will be home by sunset."

  $s \rightarrow t$
- Show the conclusion that "we will be home by sunset."

  t

- p: It is sunny this afternoon.
- q: It is colder than yesterday.
- r: We will go swimming.
- s: We will take a canoe trip.
- t: We will be home by sunset.

Using Rules of Inference to Build Arguments

- p: It is sunny this afternoon.
- q: It is colder than yesterday.
- r: We will go swimming.
- s: We will take a canoe trip.
- t: We will be home by sunset.

Premises: $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$

Conclusion: t

Using Rules of Inference to Build Arguments

- p: It is sunny this afternoon.
- q: It is colder than yesterday.
- r: We will go swimming.
- s: We will take a canoe trip.
- t: We will be home by sunset.

Premises: $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$

Conclusion: t

Step	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens using (6) and (7)

Rules of Inference for Quantified Statements

- **Universal Instantiation** (UI)

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

- **Universal Generalization** (UG)

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

- **Existential Instantiation** (EI)

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

- **Existential Generalization** (EG)

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

Applying Rules of Inference for Quantified Statements

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

Applying Rules of Inference for Quantified Statements

- "A student in this class has not read the book."
- "Everyone in this class passed the first exam."
- Show the conclusion that "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.
- Domain of x: all students

Applying Rules of Inference for Quantified Statements

- "A student in this class has not read the book."

  $\exists x(C(x) \land \neg B(x))$
- "Everyone in this class passed the first exam."

  $\forall x(C(x) \to P(x))$
- Show the conclusion that "Someone who passed the first exam has not read the book."

  $\exists x(P(x) \land \neg B(x))$
- $C(x)$: x is in this class.
- $B(x)$: x has read the book.
- $P(x)$: x passed the first exam.
- Domain of x: all students

Applying Rules of Inference for Quantified Statements

- $C(x)$: x is in this class.
- $B(x)$: x has read the book.
- $P(x)$: x passed the first exam.
- Domain of x: all students

Premises: $\exists x(C(x) \wedge \neg B(x))$, $\forall x(C(x) \rightarrow P(x))$

Conclusion: $\exists x(P(x) \wedge \neg B(x))$

Applying Rules of Inference for Quantified Statements

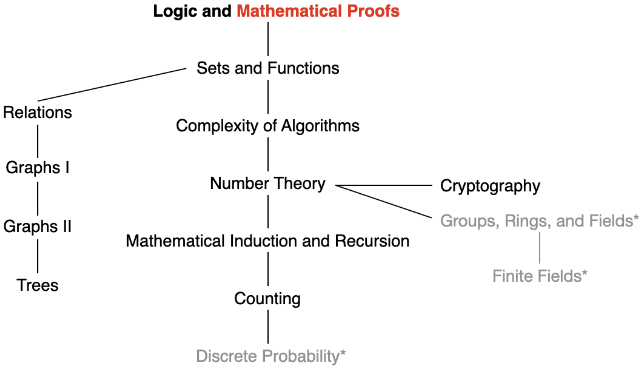
- $C(x)$: x is in this class.
- $B(x)$: x has read the book.
- $P(x)$: x passed the first exam.
- Domain of x: all students

Premises: $\exists x(C(x) \wedge \neg B(x))$, $\forall x(C(x) \to P(x))$

Conclusion: $\exists x(P(x) \wedge \neg B(x))$

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

This Lecture



Mathematical Proofs: Rules of inference, introduction to proofs

Proofs

A proof is a valid argument that establishes the truth of a mathematical statement. (Note: the truth of all its premises implies that the conclusion is true.)

Proofs

A proof is a valid argument that establishes the truth of a mathematical statement. (Note: the truth of all its premises implies that the conclusion is true.)

Premises:

- hypotheses of the theorem
- axioms assumed to be true
- previously proven theorems or lemmas

Conclusion:

- the truth of the statement

Proofs

A proof is a valid argument that establishes the truth of a mathematical statement. (Note: the truth of all its premises implies that the conclusion is true.)

Premises:

- hypotheses of the theorem
- axioms assumed to be true
- previously proven theorems or lemmas

Conclusion:

- the truth of the statement

- Axiom: a statement or proposition which is regarded as being established.
- Theorem: a statement that can be shown to be true.
- Lemma: a statement that can be proved to be true, and is used in proving a theorem or proposition.

Proofs

A proof is a valid argument that establishes the truth of a mathematical statement. (Note: the truth of all its premises implies that the conclusion is true.)

Premises:

- hypotheses of the theorem
- axioms assumed to be true
- previously proven theorems or lemmas

Conclusion:

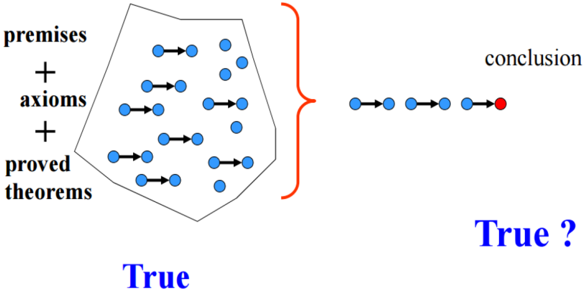
- the truth of the statement

Using rules of inference

- Axiom: a statement or proposition which is regarded as being established.
- Theorem: a statement that can be shown to be true.
- Lemma: a statement that can be proved to be true, and is used in proving a theorem or proposition.

Formal Proofs

Formal proofs: steps follow logically from the set of premises, axioms, lemmas, and other theorems.



Informal Proofs

Step	Reason
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	Existential instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	Existential generalization from (8)

In practice, **informal proofs:** steps are not expressed in any formal language of logic; steps may be skipped; the axioms being assumed and the rules of inference used are not explicitly stated; ...

Methods of Proving Theorems

- **Direct proof**

  $p \to q$ is proved by showing that if p is true then q follows

Methods of Proving Theorems

- **Direct proof**

  $p \to q$ is proved by showing that if p is true then q follows
- **Proof by contrapositive**

  show the contrapositive $\neg q \to \neg p$

Methods of Proving Theorems

- **Direct proof**

  $p \to q$ is proved by showing that if p is true then q follows

- **Proof by contrapositive**

  show the contrapositive $\neg q \to \neg p$

- **Proof by contradiction**

  show that $(p \land \neg q)$ contradicts the assumptions

Methods of Proving Theorems

- **Direct proof**

  $p \to q$ is proved by showing that if p is true then q follows

- **Proof by contrapositive**

  show the contrapositive $\neg q \to \neg p$

- **Proof by contradiction**

  show that $(p \land \neg q)$ contradicts the assumptions

- **Proof by cases**

  give proofs for all possible cases

Methods of Proving Theorems

- **Direct proof**

  $p \to q$ is proved by showing that if p is true then q follows

- **Proof by contrapositive**

  show the contrapositive $\neg q \to \neg p$

- **Proof by contradiction**

  show that $(p \land \neg q)$ contradicts the assumptions

- **Proof by cases**

  give proofs for all possible cases

- **Proof of equivalence**

  $p \leftrightarrow q$ is replaced with $(p \to q) \land (q \leftarrow p)$

SUSTech Southern University of Science and Technology

Methods of Proving Theorems

- **Direct proof**

  $p \to q$ is proved by showing that if p is true then q follows

- **Proof by contrapositive**

  show the contrapositive $\neg q \to \neg p$

- **Proof by contradiction**

  show that $(p \wedge \neg q)$ contradicts the assumptions

- **Proof by cases**

  give proofs for all possible cases

- **Proof of equivalence**

  $p \leftrightarrow q$ is replaced with $(p \to q) \wedge (q \leftarrow p)$

Recall argument is a sequence of propositions that end with a conclusion, and a proof is a valid argument.
We work on propositions in proofs.

Direct Proof

$p \rightarrow q$ is proved by showing that if p is true then q follows

Example: Prove that "if n is odd, then n^2 is odd"

Direct Proof

$p \to q$ is proved by showing that if p is true then q follows

Example: Prove that "if n is odd, then n^2 is odd"

Proof:

Assume that (the hypothesis is true, i.e., n is odd)
$n = 2k + 1$ where k is an integer.
Then
$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$
Therefore, n^2 is odd.

Proof by Contrapositive

$p \to q$ is proved by showing the contrapositive $\neg q \to \neg p$

Example: Prove that "if $3n + 2$ is odd, then n is odd"

Proof by Contrapositive

$p \to q$ is proved by showing the contrapositive $\neg q \to \neg p$

Example: Prove that "if $3n + 2$ is odd, then n is odd"

Proof:

Assume that n is even, i.e., $n = 2k$, where k is an integer. Then

$3n + 2 = 3(2k) + 2 = 2(3k + 1)$.

Therefore, $3n + 2$ is even.

Proof by Contradiction

Assume that p is true but q is false (i.e., $p \wedge \neg q$). Then show a contradiction to p, or $\neg q$, or other settled results.

Example: Prove that "if $3n + 2$ is odd, then n is odd"

Proof by Contradiction

Assume that p is true but q is false (i.e., $p \land \neg q$). Then show a contradiction to p, or $\neg q$, or other settled results.

Example: Prove that "if $3n + 2$ is odd, then n is odd"

Proof:

Assume that $3n + 2$ is odd and n is even, i.e., $n = 2k$, where k is an integer. Then

$3n + 2 = 3(2k) + 2 = 2(3k + 1)$.

Thus, $3n + 2$ is even. This is a contradiction to the assumption that $3n + 2$ is odd. Therefore, n is odd.

Proof by Cases

We want to show $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$. This is equivalent to $(p_1 \to q) \wedge (p_2 \to q) \wedge ... \wedge (p_n \to q)$. Why?

Proof by Cases

We want to show $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$. This is equivalent to $(p_1 \to q) \wedge (p_2 \to q) \wedge ... \wedge (p_n \to q)$. Why?

$$
\begin{aligned}
& (p_1 \vee p_2 \vee \ldots \vee p_n) \to q \\
\equiv\ & \neg(p_1 \vee p_2 \vee \ldots \vee p_n) \vee q \\
\equiv\ & (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n) \vee q \\
\equiv\ & (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \ldots \wedge (\neg p_n \vee q) \\
\equiv\ & (p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)
\end{aligned}
$$

Proof by Cases

We want to show $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$. This is equivalent to $(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)$. Why?

$$
\begin{aligned}
& (p_1 \vee p_2 \vee \ldots \vee p_n) \to q \\
\equiv\ & \neg(p_1 \vee p_2 \vee \ldots \vee p_n) \vee q \\
\equiv\ & (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n) \vee q \\
\equiv\ & (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \ldots \wedge (\neg p_n \vee q) \\
\equiv\ & (p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)
\end{aligned}
$$

Example: Prove that "$|x||y| = |xy|$ for real numbers x, y"

SUSTech Southern University of Science and Technology

Proof by Cases

We want to show $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$. This is equivalent to $(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)$. Why?

$$
\begin{aligned}
& (p_1 \vee p_2 \vee \ldots \vee p_n) \to q \\
\equiv\ & \neg(p_1 \vee p_2 \vee \ldots \vee p_n) \vee q \\
\equiv\ & (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n) \vee q \\
\equiv\ & (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \ldots \wedge (\neg p_n \vee q) \\
\equiv\ & (p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)
\end{aligned}
$$

Example: Prove that "$|x||y| = |xy|$ for real numbers x, y"

Proof: Four cases:

- $\diamond\ x \geq 0,\ \ y \geq 0$
- $\diamond\ x \geq 0,\ \ y < 0$
- $\diamond\ x < 0,\ \ y \geq 0$
- $\diamond\ x < 0,\ \ y < 0$

Proof of Equivalences

To prove $p \leftrightarrow q$, show $(p \rightarrow q) \wedge (q \leftarrow p)$

Example: Prove that "An integer n is odd if and only if n^2 is odd"

Proof of Equivalences

To prove $p \leftrightarrow q$, show $(p \rightarrow q) \wedge (q \leftarrow p)$

Example: Prove that "An integer n is odd if and only if n^2 is odd"

Proof:

◇ proof of $p \rightarrow q$: direct proof
◇ proof of $q \rightarrow p$: proof by contrapositive

Vacuous Proof

To prove $p \to q$, suppose that p (the hypothesis) is always false, then $p \to q$ is always true.

Example: $P(n)$: if $n > 1$, then $n^2 > n$. Show P(0) is true.

Vacuous Proof

To prove $p \to q$, suppose that p (the hypothesis) is always false, then $p \to q$ is always true.

Example: $P(n)$: if $n > 1$, then $n^2 > n$. Show P(0) is true.

Proof: Since the premise $0 > 1$ is always false. Thus $P(0)$ is true.

Vacuous Proof

To prove $p \rightarrow q$, suppose that p (the hypothesis) is always false, then $p \rightarrow q$ is always true.

Example: $P(n)$: if $n > 1$, then $n^2 > n$. Show P(0) is true.

Proof: Since the premise $0 > 1$ is always false. Thus $P(0)$ is true.

Vacuous proofs are often used to establish special cases of theorems that state that a conditional statement is true for all positive integers.

Trivial Proof

To prove $p \to q$, suppose that q (the conclusion) is always true, then $p \to q$ is always true.

Example: $P(n)$: if $a \geq b$, then $a^n \geq b^n$. Show $P(0)$ is true.

Trivial Proof

To prove $p \to q$, suppose that q (the conclusion) is always true, then $p \to q$ is always true.

Example: $P(n)$: if $a \geq b$, then $a^n \geq b^n$. Show $P(0)$ is true.

Proof: Since the conclusion $a^0 \geq b^0$ is always true for any value of a and b. Thus $P(0)$ is true.

Proofs with Quantifiers

Universal quantified statements

- Prove the property holds for all examples
  - proof by cases to divide the proof into different parts

- Disprove universal statements
  - existential quantified statements
  - counterexamples

Proofs with Quantifiers

Existential quantified statements

- Constructive
  - find a specific example to show the statement holds
- Nonconstructive
  - any method other than the constructive method
  - e.g., proof by contradiction

- Disprove: there does not exist any ...
  - universal quantified statements

Proofs with Quantifiers

Uniqueness proofs: assert the existence of a unique element with a particular property.

- Existence: We show that an element x with the desired property exists.
- Uniqueness: We show that if $y \neq x$, then y does not have the desired property. Or, if y has the desired property, then $y = x$.

Example

Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution:

Example

Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution:

- Existence: The real number $r = -b/a$ is a solution of $ar + b = 0$. Consequently, a real number r exists for which $ar + b = 0$.

Example

Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution:

- Existence: The real number $r = -b/a$ is a solution of $ar + b = 0$. Consequently, a real number r exists for which $ar + b = 0$.
- Uniqueness: Suppose that s is a real number such that $as + b = 0$. Then, $ar + b = as + b$, where $r = -b/a$. Dividing both sides of this last equation by a, which is nonzero, we see that $r = s$.

Proof Exercise

Prove that $\sqrt{2}$ is irrational. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

Proof Exercise

Prove that $\sqrt{2}$ is irrational. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

Proof: Suppose that $\sqrt{2}$ is rational. Then, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (so that the fraction a/b is in lowest terms.)

Proof Exercise

Prove that $\sqrt{2}$ is irrational. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

Proof: Suppose that $\sqrt{2}$ is rational. Then, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (so that the fraction a/b is in lowest terms.)

Since $\sqrt{2} = a/b$, it follows that $2b^2 = a^2$. By the definition of an even integer, it follows that a^2 is even, so a is even (see Exercise 16).

Proof Exercise

Prove that $\sqrt{2}$ is irrational. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

Proof: Suppose that $\sqrt{2}$ is rational. Then, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (so that the fraction a/b is in lowest terms.)

Since $\sqrt{2} = a/b$, it follows that $2b^2 = a^2$. By the definition of an even integer, it follows that a^2 is even, so a is even (see Exercise 16).

Since a is even, $a = 2k$ for some integer k. Thus, $b^2 = 2k^2$. This implies that b^2 is even, so b is even.

Proof Exercise

Prove that $\sqrt{2}$ is irrational. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

Proof: Suppose that $\sqrt{2}$ is rational. Then, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (so that the fraction a/b is in lowest terms.)

Since $\sqrt{2} = a/b$, it follows that $2b^2 = a^2$. By the definition of an even integer, it follows that a^2 is even, so a is even (see Exercise 16).

Since a is even, $a = 2k$ for some integer k. Thus, $b^2 = 2k^2$. This implies that b^2 is even, so b is even.

As a result, a and b have a common factor 2, which contradicts our assumption.

SUSTech Southern University of Science and Technology

Proof Exercise

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof:

Proof Exercise

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof: (by contraposition)

Proof Exercise

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof: (by contraposition)

- Assume that the conclusion of the conditional statement "if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$." is false.
- That is, assume that $a > \sqrt{n}$ and $b > \sqrt{n}$. (why?)
- Then, $ab > n$, that is $ab \neq n$.

Proof Exercise

Prove that there are infinitely many prime numbers.

Proof Exercise

Prove that there are infinitely many prime numbers.

Proof: Suppose that there are only a finite number of primes. Then, there exists a prime number p that is the largest of all the prime numbers. Also, we can list the prime numbers in ascending order: $2, 3, 5, 7, 11, ..., p$

SUSTech Southern University of Science and Technology

Proof Exercise

Prove that there are infinitely many prime numbers.

Proof: Suppose that there are only a finite number of primes. Then, there exists a prime number p that is the largest of all the prime numbers. Also, we can list the prime numbers in ascending order: $2, 3, 5, 7, 11, ..., p$

Let $n = (2 \times 3 \times 5 \times \cdots \times p) + 1$. Then, $n > 1$, and n cannot be divided by any prime number in the list above. This means that n is also a prime.

Proof Exercise

Prove that there are infinitely many prime numbers.

Proof: Suppose that there are only a finite number of primes. Then, there exists a prime number p that is the largest of all the prime numbers. Also, we can list the prime numbers in ascending order: $2, 3, 5, 7, 11, ..., p$

Let $n = (2 \times 3 \times 5 \times \cdots \times p) + 1$. Then, $n > 1$, and n cannot be divided by any prime number in the list above. This means that n is also a prime.

Clearly, n is larger than all the primes in the list above. This is contrary to the assumption that all primes are in the list.

Proof Exercise

Show that there exist irrational numbers x and y such that x^y is rational.

Proof Exercise

Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

Proof Exercise

Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have two irrational numbers $x = \sqrt{2}$ and $y = \sqrt{2}$ with $x^y = \sqrt{2}^{\sqrt{2}}$ rational.

Proof Exercise

Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have two irrational numbers $x = \sqrt{2}$ and $y = \sqrt{2}$ with $x^y = \sqrt{2}^{\sqrt{2}}$ rational.

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We have $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ is rational.

Proof Exercise

Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have two irrational numbers $x = \sqrt{2}$ and $y = \sqrt{2}$ with $x^y = \sqrt{2}^{\sqrt{2}}$ rational.

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We have $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ is rational.

Note that although we do not know which case works, we know that one of the two cases has the desired property.

Next Lecture