Discrete Mathematics
Lec 2: Logic and Proofs:Part 2

馬誠佑

More about quantifier

- The uniqueness quantifier: ∃!
  $\exists! \, xP(x) = \text{“}There\ exists\ exactlty\ one\ x\ such\ that\ P(x)\ is\ true.\text{”}$

- $\forall x \in U, P(x) \equiv \forall x\big(x \in U \wedge P(x)\big)$

  $\exists x \in U, P(x) \equiv \exists x\big(x \in U \wedge P(x)\big)$

- $\forall x \forall y P(x,y) \equiv \forall y \forall x P(x,y) \equiv \forall xy \; P(x,y)$
  $\exists x \exists y P(x,y) \equiv \exists y \exists x P(x,y) \equiv \exists xy \; P(x,y)$

Binding and free variables

Statement	Binding and Free variables
$P(x)$	x: free variable
$P(x, y)$	x, y: free variable
$\forall x P(x)$	x: bound
$\forall x P(x, y)$	x: bound, y: free variable
$\forall x \exists y P(x, y)$	x, y: bound

Ex:

Please compare the statements below:

- $\exists x\big(S(x) \wedge M(x)\big)\ v.s.\ (\exists x S(x)) \wedge M(x)$ v.s. $\exists x S(x) \wedge M(x)$
- $\exists y S(y) \wedge M(x)\ v.s. \exists y\big(S(y) \wedge M(x)\big)$

Are the Universal and Existential Quantifiers Commutable?

- Let $P(x) =$ $\text{“}x\ likes\ y.\text{”}\ What\ are\ the\ meanings\ of\ logic\ expressions\ below?$
- $\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y) \equiv \forall x y P(x, y)$
- $\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y) \equiv \exists x y P(x, y)$
- $\forall x \exists y P(x, y)$
- $\forall y \exists x P(x, y)$
- $\exists y \forall x P(x, y)$
- $\exists x \forall y P(x, y)$

Example

- Show that $\neg\forall x\big(P(x) \to Q(x)\big) \equiv \exists x\big(P(x) \wedge \neg Q(x)\big)$

Pf:

$$\neg\forall x\big(P(x) \to Q(x)\big) \equiv \neg\forall x\big(\neg P(x) \vee Q(x)\big)$$
$$\equiv \exists x \neg\big(\neg P(x) \vee Q(x)\big)$$
$$\equiv \exists x\Big(\neg\big(\neg P(x)\big) \wedge \neg Q(x)\Big)$$
$$\equiv \exists x\big(P(x) \wedge \neg Q(x)\big)$$

Example

- Express the statement “Every student in this class has studied Java.”

Let $P(x) = \text{“}x\ has\ studied\ Java.\text{”}$ and $U = \{x: x\ is\ a\ student\ in\ this\ class\}. Then,$

$$\forall x \in U, P(x).$$

If $U\ is\ all\ people, then\ let\ Q(x) = \text{“}x\ is\ a\ student\ in\ the\ class.\text{”}$

$$Then, \forall x\big(Q(x) \rightarrow P(x)\big).$$

Lewis Carroll Example

The first two are called *premises* and the third is called the *conclusion*.

1. "All lions are fierce."
2. "Some lions do not drink coffee."
3. "Some fierce creatures do not drink coffee."

Here is one way to translate these statements to predicate logic. Let P(x), Q(x), and R(x) be the propositional functions "x is a lion," "x is fierce," and "x drinks coffee," respectively.

1. $\forall X \ (P(X) \rightarrow Q(X))$
2. $\exists X \ (P(X) \wedge \neg R(X))$
3. $\exists X \ (Q(X) \wedge \neg R(X))$

由1知道任一X P(X)->Q(X)
將 2中P(X)換成Q(X) 得3

Later we will see how to prove that the conclusion follows from the premises

System Specification Example

Predicate logic is used for specifying properties that systems must satisfy.

For example, translate into predicate logic:

- "Every mail message larger than one megabyte will be compressed."
- "If a user is active, at least one network link will be available."

Decide on predicates and domains (left implicit here) for the variables:

- Let $L(m, y)$ be "Mail message m is larger than y megabytes."
- Let $C(m)$ denote "Mail message m will be compressed."
- Let $A(u)$ represent "User u is active."
- Let $S(n, x)$ represent "Network link n is state x.

Now we have:

$$\forall m\big(L(m,1) \rightarrow C(m)\big)$$

$$\exists u\ A(u) \rightarrow \exists n\ S(n,\ available)$$

Example

- Express the negations of each of these statements so that all negation symbols immediately precede predicates.
  1. $\forall x \exists y \forall z T(x, y, z)$
  2. $\forall x \exists y P(x, y) \vee \forall x \exists y Q(x, y)$
  3. $\forall x \exists y P(x, y) \wedge \exists z R(x, y, z)$
  4. $\forall x \exists y P(x, y) \rightarrow Q(x, y)$

$\neg(\forall x \exists y \forall z T(x, y, z)) \equiv \exists x \neg(\exists y \forall z T(x, y, z)) \equiv$
$\exists x \forall y \neg(\forall z T(x, y, z)) \equiv \exists x \forall y \exists z \neg T(x, y, z))$

Rules of inferences

- $P(x) \rightarrow \neg Q(x)$ …Premises

….$P(x)\ is\ true$ …Premises

….$\neg Q(x)$ …Conclusion

- Ex:

  We have the two premises:

  - "All men are mortal."
  - "Socrates is a man."

  And the conclusion:

  - "Socrates is mortal."

  How do we get the conclusion from the premises?

The Argument

We can express the premises (above the line) and the conclusion (below the line) in predicate logic as an argument:

$$\frac{\begin{array}{c}\forall x\left(Man\left(x\right)\rightarrow Mortal\left(x\right)\right)\\ Man\left(Socrates\right)\end{array}}{\therefore\quad Mortal\left(Socrates\right)}$$

We will see shortly that this is a valid argument.

P_1

P_2

(∧) P_3

Q

} Premises

Conclusion

$(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \rightarrow Q$

$p \rightarrow q$

∧ $q \rightarrow r$

$p \rightarrow r$

} Premises

Conclusion

$$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$$
$$\equiv (\neg p \vee q) \wedge (\neg q \vee r) \rightarrow (\neg p \vee r)$$
$$\equiv (\neg p \wedge \neg q) \vee (\neg p \wedge r) \vee (\cancel{q \wedge \neg q}) \vee (q \wedge r) \rightarrow (\neg p \vee r)$$
$$\equiv \neg[(\neg p \wedge \neg q) \vee (\neg p \wedge r) \vee (q \wedge r)] \vee ((\neg p \vee r))$$
$$\equiv [(p \vee q) \wedge (p \vee \neg r) \wedge (\neg q \vee \neg r)] \vee (\neg p \vee r)$$
$$\equiv T \wedge T \wedge T \equiv T$$

分配律進去恆真

Valid Arguments[1]

We will show how to construct valid arguments in two stages; first for propositional logic and then for predicate logic. The rules of inference are the essential building block in the construction of valid arguments.

1. Propositional Logic

   Inference Rules

2. Predicate Logic

   Inference rules for propositional logic plus additional inference rules to handle variables and quantifiers.

Arguments in Propositional Logic

A *argument* in propositional logic is a sequence of propositions. All but the final proposition are called *premises*. The last statement is the *conclusion*.

The argument is valid if the premises imply the conclusion. An *argument form* is an argument that is valid no matter what propositions are substituted into its propositional variables.

If the premises are $p_1, p_2, \ldots, p_n$ and the conclusion is q then

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$$ is a tautology.

Inference rules are all argument simple argument forms that will be used to construct more complex argument forms.

Rules of Inference for Propositional Logic: Modus Ponens

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

Corresponding Tautology:

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

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

Example:

Let p be "It is snowing."

Let q be "I will study discrete math."

"If it is snowing, then I will study discrete math."

"It is snowing."

"Therefore , I will study discrete math."

Modus Tollens

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

Corresponding Tautology:

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

Example:

Let p be “it is snowing.”

Let q be “I will study discrete math.”

“If it is snowing, then I will study discrete math.”

“I will not study discrete math.”

“Therefore , it is not snowing.”

Hypothetical Syllogism

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

Corresponding Tautology:

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

Example:

Let *p* be “it snows.”

Let *q* be “I will study discrete math.”

Let *r* be “I will get an A.”

“If it snows, then I will study discrete math.”

“If I study discrete math, I will get an A.”

“Therefore , If it snows, I will get an A.”

Disjunctive Syllogism

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

Corresponding Tautology:

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

Example:

Let p be "I will study discrete math."

Let q be "I will study English literature."

"I will study discrete math or I will study English literature."

"I will not study discrete math."

"Therefore , I will study English literature."

Addition

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

Corresponding Tautology:

$$p \rightarrow (p \vee q)$$

Example:

Let p be “I will study discrete math.”

Let q be “I will visit Las Vegas.”

“I will study discrete math.”

“Therefore, I will study discrete math or I will visit

Las Vegas.”

Simplification

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

Corresponding Tautology:

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

Example:

Let p be "I will study discrete math."

Let q be "I will study English literature."

"I will study discrete math and English literature"

"Therefore, I will study discrete math."

Conjunction

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

Corresponding Tautology:

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

Example:

Let p be "I will study discrete math."

Let q be "I will study English literature."

"I will study discrete math."

"I will study English literature."

"Therefore, I will study discrete math and I will study English literature."

Resolution

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

Resolution plays an important role in AI and is used in Prolog.

Corresponding Tautology:

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

$$\equiv \neg[(\neg p \vee r) \wedge (p \vee q)] \vee (q \vee r)$$
$$\equiv \neg[(\neg p \wedge p) \vee (\neg p \wedge q) \vee (r \wedge p) \vee (r \wedge q)] \vee (q \vee r)$$
$$\equiv [(p \vee \neg q) \wedge (\neg r \vee \neg p) \wedge (\neg r \vee \neg q)] \vee (q \vee r)$$
$$\equiv \mathrm{T} \wedge T \wedge T \equiv T$$

分配律進去恆真

Example:

Let *p* be “I will study discrete math.”

Let *r* be “I will study English literature.”

Let q be “I will study databases.”

“I will not study discrete math or I will study English literature.”

“I will study discrete math or I will study databases.”

“Therefore, I will study databases or I will study English literature.”

Rules of Inferences

Rules	Tautology	Name
$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$	$(p \wedge (p \to q)) \to q$	Modus Ponens
$\begin{array}{l} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus Tollens
$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical Syllogism
$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$	$(\neg p \wedge (p \vee q)) \to q$	Disjunctive Syllogism
$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$	$p \to (p \vee q)$	Addition
$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$	$(p \wedge q) \to p$	Simplification
$\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$\begin{array}{l} \neg p \vee r \\ p \vee q \\ \hline \therefore q \vee r \end{array}$	$((\neg p \vee r) \wedge (p \vee q)) \to (q \vee r)$	Resolution

Another Proof

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

Pf. $(\neg p \vee r) \equiv p \rightarrow r$

$(p \vee q) \equiv \neg p \rightarrow q \equiv \neg q \rightarrow p$

$\neg q \rightarrow r \equiv q \vee r$

Example

- State which rule of inference is used in the argument:

  - “If it rains today, then we will not have a barbecue today.”
  - ”If we do not have a barbecue todatay, then we will have a barbecue tomorrow.”
  - “Therefore, if it rains today, then we will have a barbecue tomorrow.”

Sol:

Let p = “It is raining today.”, q = “We will not have barbecue today”, and r = “We will have a barbecue tomorrow.”

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

Hence, this argument is a hypothetical syllogism.

Rules	Tautology	Name
$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus Ponens
$\begin{array}{l} p \rightarrow q \\ \neg q \\ \hline \therefore \neg p \end{array}$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus Tollens
$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical Syllogism
$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$	$(\neg p \wedge (p \vee q)) \rightarrow q$	Disjunctive Syllogism
$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$	$p \rightarrow (p \vee q)$	Addition
$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$	$(p \wedge q) \rightarrow p$	Simplification
$\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\begin{array}{l} \neg p \vee r \\ p \vee q \\ \hline \therefore q \vee r \end{array}$	$((\neg p \vee r) \wedge (p \vee q)) \rightarrow (q \vee r)$	Resolution

Example

- Show that the premises “If you send me an e-mail message, then I will finish writing the program,” “If you do not send me an e-mail message, then I will go to sleep early,” and “If I go to sleep early, then I will wake up feeling refreshed” lead to the conclusion “If I do not finish writing the program, then I will wake up feeling refreshed.”
- *Solution:* Let p = “You send me an e-mail message,” q =“I will finish writing the program,” r = “I will go to sleep early,” and s= “I will wake up feeling refreshed.”
- Then the premises are
  1. $p \rightarrow q$,
  2. $\neg p \rightarrow r$
  3. $r \rightarrow s$
- conclusion is $\neg q \rightarrow s$.

Step	**Reason**
1. $p \rightarrow q$	Premise
2. $\neg q \rightarrow \neg p$	Contrapositive of (1)
3. $\neg p \rightarrow r$	Premise
4. $\neg q \rightarrow r$	Hypothetical syllogism using (2) and (3)
5. $r \rightarrow s$	Premise
6. $\neg q \rightarrow s$	Hypothetical syllogism using (4) and (5)

Rules	Tautology	Name
$\frac{p \rightarrow q,\ p}{\therefore q}$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus Ponens
$\frac{p \rightarrow q,\ \neg q}{\therefore \neg p}$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus Tollens
$\frac{p \rightarrow q,\ q \rightarrow r}{\therefore p \rightarrow r}$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical Syllogism
$\frac{p \vee q,\ \neg p}{\therefore q}$	$(\neg p \wedge (p \vee q)) \rightarrow q$	Disjunctive Syllogism
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p,\ q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{\neg p \vee r,\ p \vee q}{\therefore q \vee r}$	$((\neg p \vee r) \wedge (p \vee q)) \rightarrow (q \vee r)$	Resolution

- $q \rightarrow p$為$p \rightarrow q$的逆命題; 換位命題**(converse)**
- $\neg p \rightarrow \neg q$ 為$p \rightarrow q$的反命題; 異質命題 **(inverse)**
- $\neg q \rightarrow \neg p$為$p \rightarrow q$的質位互換命題 **(contrapositive)**

Example

Rules	Tautology	Name
$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$	$(p \wedge (p \to q)) \to q$	Modus Ponens
$\begin{array}{l} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus Tollens
$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical Syllogism
$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$	$(\neg p \wedge (p \vee q)) \to q$	Disjunctive Syllogism
$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$	$p \to (p \vee q)$	Addition
$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$	$(p \wedge q) \to p$	Simplification
$\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$\begin{array}{l} \neg p \vee r \\ p \vee q \\ \hline \therefore q \vee r \end{array}$	$((\neg p \vee r) \wedge (p \vee q)) \to (q \vee r)$	Resolution

- With these hypotheses:
  "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."
- Using the inference rules, construct a valid argument for the conclusion:
  "We will be home by sunset."
- **Solution**:

1. Choose propositional variables:
   p : "It is sunny this afternoon." r : "We will go swimming." t : "We will be home by sunset."
   q : "It is colder than yesterday." s : "We will take a canoe trip."
2. Translation into propositional logic:

Hypotheses: $\neg p \wedge q,\ r \to p,\ \neg r \to s,\ s \to t$

Conclusion: t

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

Fallacies

- $[(p \rightarrow q) \wedge q\ ] \rightarrow p$ is not a tautology

$p \rightarrow q$

q

---------- *is wrong*

$\therefore p$

- $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ is not a tautology.

$p \rightarrow q$

$\neg p$

---------- *is wrong*

$\therefore \neg q$

Rules of Inference for Quantified Statements

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\forall x P(x)$ $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$ $\therefore P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore \exists x P(x)$	Existential generalization

Universal Instantiation (UI)

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

Example:

Our domain consists of all dogs and Fido is a dog.

“All dogs are cuddly.”

“Therefore, Fido is cuddly.”

Universal Generalization (UG)

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

Used often implicitly in Mathematical Proofs.

Existential Instantiation (EI)

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

Example:

"There is someone who got an A in the course."

"Let's call her *a* and say that *a* got an A"

Existential Generalization (EG)

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

Example:

"Michelle got an A in the class."

"Therefore, someone got an A in the class."

Using Rules of Inference[1]

Example 1: Using the rules of inference, construct a valid argument to show that

"John Smith has two legs"

is a consequence of the premises:

"Every man has two legs." "John Smith is a man."

Solution: Let $M(x)$ denote "x is a man" and $L(x)$ " x has two legs" and let John Smith be a member of the domain.

Valid Argument:

Step	**Reason**
1. $\forall x\left(M\left(x\right)\rightarrow L\left(x\right)\right)$	Premise
2. $M\left(J\right)\rightarrow \mathrm{L}\left(J\right)$	UI from $\left(1\right)$
3. $M\left(J\right)$	Premise
4. $L\left(J\right)$	Modus Ponens using $\left(2\right)$ and $\left(3\right)$

Using Rules of Inference 2

Example 2: Use the rules of inference to construct a valid argument showing that the conclusion

"Someone who passed the first exam has not read the book."

follows from the premises

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

"Everyone in this class passed the first exam."

Solution: Let $C(x)$ denote "x is in this class," $B(x)$ denote "x has read the book," and $P(x)$ denote "x passed the first exam."

First we translate the premises and conclusion into symbolic form.

$$\exists x\big(C(x) \wedge \neg B(x)\big)$$

$$\frac{\forall x\big(C(x) \rightarrow P(x)\big)}{\therefore \exists x\big(P(x) \wedge \neg B(x)\big)}$$

Continued on next slide →

Using Rules of Inference 3

Valid Argument:

Step	Reason
1. $\exists x\left(C\left(x\right)\wedge\neg B\left(x\right)\right)$	Premise
2. $C\left(a\right)\wedge\neg\mathrm{B}\left(a\right)$	EI from $\left(1\right)$
3. $C\left(a\right)$	Simplification from $\left(2\right)$
4. $\forall x\left(C\left(x\right)\rightarrow P\left(x\right)\right)$	Premise
5. $C\left(a\right)\rightarrow P\left(a\right)$	UI from $\left(4\right)$
6. $P\left(a\right)$	MP from $\left(3\right)$ and $\left(5\right)$
7. $\neg B\left(a\right)$	Simplification from $\left(2\right)$
8. $P\left(a\right)\wedge\neg B\left(a\right)$	Conj from $\left(6\right)$ and $\left(7\right)$
9. $\exists x\left(P\left(x\right)\wedge\neg B\left(x\right)\right)$	EG from $\left(8\right)$

Terminology

- Theorem: A theorem is a statement that can be shown to be true.
- Proposition: Less important theorems are called propositions.
- Proof: A proof is a valid argument that established the truth of a theorem.
- Axiom (原則, 公理): Statements that we assume to be true.
- Lemma（弓|理）: A less important theorem that is helpful in the proof of other results.
- Corollary（推論）: A theorem that can be established directly from a theorem that has been proved.
- Conjecture（推測,猜想）: A statement that is being proposed to be a true statement.

How to Prove Conditional Statements

- Direct proof
- Proof by contraposition ($\neg q \rightarrow \neg p$)
- Proof by contradiction
- Vacuous and trivial proof

$$p \rightarrow q$$

Direct proofs

- Def: The integer *n* is *even* if there exists an integer *k* such that *n* = 2*k*, and *n* is *odd* if there exists an integer *k* such that *n* = 2*k* + 1. (Note that every integer is either even or odd, and no integer is both even and odd.)

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

Pf.

$\forall n \in Z$, $\forall n$ ($P(n) \rightarrow Q(n)$), where $P(n)$ is "n is an odd integer" and $Q(n)$ is "$n^2$is odd.

Assume n is an odd number. According to the definition, there exists an integer k such that n = 2k+1. Then,

$n^2 = (2k+1)^2 = 4k^2 + 4\mathrm{k} + 1 = 2(2k^2 + 2\mathrm{k}) + 1$

Proof by Contraposition

- $p \rightarrow q \equiv \neg q \rightarrow \neg p$

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

Pf. Assume n is not odd. Then, n is even. There exists an integer k such that n=2k.

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

Since 3k+1 is an integer, 3n+2 is even. So, the premise is not true. Therefore, the theorem is proved.

Example

- The real number r is rational if there exists integers p and q with q$\neq 0$ such that r = p/q. A real number that is not rational is called irrational.

Prove that the sum of two rational numbers is rational.

$$\forall x, y, R(x) \wedge R(Y) \rightarrow R(x + y)$$

Assume R(x) and R(y) are true. (premise)

$$R(x) \rightarrow \exists p, q \neq 0 \; such \; that \; x = \frac{p}{q}$$

$$R(y) \rightarrow \exists r, s \neq 0 \; such \; that \; y = \frac{r}{s}$$

$x + y = \frac{p}{q} + \frac{r}{s} = \frac{ps+rq}{qs}$, ps+rq and qs are integer and qs $\neq 0$, $\therefore x + y$ is rational.

Example

- Prove that if *n* is an integer and n^2 is odd, then *n* is odd.

Pf.

We prove $\neg odd(n) \rightarrow \neg odd(n^2)$. Assume $\neg odd(n)$ is true => n is even. Then, there exists k such that n = 2k.

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

Since $2k^2$ is an integer n^2 is even. Therefore $\neg odd(n^2)$ is true.

Vacuous and trivial proofs

- To prove $p \rightarrow q$ is true, we can
  - Show p is false (vacuous proof); or
  - Show q is true (trivial proof)
- Ex (Vacuous proof)

Let P(n)="if n>1, then $n^2 > n$". Prove P(0) is true.

P(0)="if 0>1, then $0^2 > 0$"

In the conditional statement, the premise "0>1" is false, so P(0) is true.

Example (Trivial proof)

- Let P(n)="if a and b are positive integers with $a \geq b, then\ a^n \geq b^n$."

Show that P(0) is true.

Pf.

P(0) = "if a and b are positive integers with $a \geq b, then\ a^0 \geq b^0$."

Since a^0=1 and b^0=1, $a^0 \geq b^0$ is true. So P(0) is true.

Proof by Contradiction

- If we want to prove p is true, we first assume $\neg p$. Then, by applying rules of inference, we can get some contradiction ($\neg p$ is False). Since $\neg p \rightarrow F$ is true, we can say p is T.

- Suppose we want to prove that a statement *p* is true. Furthermore, suppose that we can find a contradiction *q* such that ¬*p* → *q* is true. Because *q* is false, but ¬*p* → *q* is true, we can conclude that ¬*p* is false, which means that *p* is true.

Example (Proof by Contradiction)

- Prove that "$\sqrt{2}$ is irrational" by contradiction.

Pf.

Let *p* be the proposition "$\sqrt{2}$ is irrational." To start a proof by contradiction, we suppose that ¬*p* is true. Note that ¬*p* is the statement "It is not the case that $\sqrt{2}$ is irrational," which says that $\sqrt{2}$ is rational. We will show that assuming that ¬*p* is true leads to a contradiction.

Assume $\sqrt{2}$ is not irrational ($\sqrt{2}$ is rational). There exists integers r, s$\neq 0$ such that $\sqrt{2}$ = r/s (Beside, we can assume r and s are both coprime)

$$r^2 = 2s^2$$

Since r^2 is even, r is even. ($\mathrm{E}(r^2) \rightarrow E(r)$). Assume r = 2k, $(2k)^2 = 2s^2$

=> $s^2 = 2k^2$. Since s^2 is even, s is even. ($\mathrm{E}(s^2) \rightarrow E(s)$). 2|r and 2|s, imply r, s are not coprime. There is a contradiction. => $\sqrt{2}$ is rational is not true, then theorem proved.

Mistakes in proofs

- What is wrong with this famous supposed "proof" that 1 = 2?
  "Proof": We use these steps, where *a* and *b* are two equal positive integers.

Step	**Reason**
$a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by *a* Subtract b^2 from both sides of (2)
3. $a^2 - b^2 = ab - b^2$	Factor both sides of (3)
4. $(a-b)(a+b) = b(a-b)$	Divide both sides of (4) by $a - b$
5. $a+b=b$	Replace *a* by *b* in(5) because$a=b$ and simplify
6. $2b = b$	Divide both sides of (6) by *b*
7. 2 = 1	

- *Solution:* Every step is valid except for step 5, where we divided both sides by $a - b$. The error is that $a - b$ equals zero; division of both sides of an equation by the same quantity is valid as long as this quantity is not zero.

Mistakes in proofs

- Prove that if n is not positive, then n^2 is not positive.

Pf.

It is known that "if n is positive, then n^2 $is\ positive$." Now, n is not positive, we can conclude that n^2 is not positive.

$$p \rightarrow q$$
$$\neg p$$
$$\therefore \neg q$$

Proof by cases (Exhaustive proof)

- To prove a conditional state of the form

$(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$, based on the logical equivalence

$(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q \equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$

We may prove

$\forall i = 1,2, \ldots,\text{n}\ \ p_i \rightarrow q$

Therefore, to prove $p \rightarrow q$, if we knows

$p \equiv p_1 \vee p_2 \vee \cdots \vee p_n$

Then, we can show

$\forall i = 1,2, \ldots,\text{n}\ \ p_i \rightarrow q$

Example

- Show that there are no solutions in integers x and y of $x^2 + 3y^2 = 8$

Solution: We can quickly reduce a proof to checking just a few simple cases because $x^2 > 8$ when $|x| \geq 3$ and $3y^2 > 8$ when $|y| \geq 2$. This leaves the cases when x equals $-2, -1, 0, 1$, or 2 and y equals $-1, 0$, or 1. We can finish using an exhaustive proof. To dispense with the remaining cases, we note that possible values for x^2 are 0, 1, and 4, and possible values for $3y^2$ are 0 and 3, and the largest sum of possible values for x^2 and $3y^2$ is 7. Consequently, it is impossible for $x^2 + 3y^2 = 8$ to hold when x and y are integers. ◀

Without loss of generality (不失一般性)
WLOG

An Common Inference Errors with Exhaustive Proof

- $p \equiv$ "$p_1 \vee p_2 \vee \cdots \vee p_n$"
- The exhaustive proof will be invalid, if only a subset of $p_1, \ldots, p_n$ is considered.
- If x is a real number, then x^2 is a positive real number.

Pf. "x is a real number" $\equiv$ "$x\ is\ positive$" $\vee$ "$x\ is\ negative$" $\vee$ "$x = 0$"

$p_1 = x\ is\ positive, p_2 = x\ is\ negative, q = x^2\ is\ positive.$

Case 1: if p_1, x>0. So, x^2>0.

Case 2: if p_2, x<0. So, x^2>0.

Therefore, the theorem is proved…..?

Existential Proofs

- To prove the statement $\exists x P(x), we\ can$
- Constructive proof: Find an element a, such that $P(a)\ is\ true$.
- Nonconstructive proof: We don't provide an element a, but prove the truth in some other way.

Ex.

There is a positive integer that can be written as the sum of cube of positive integers in two different way.

Pf.

1729 =$10^3 + 9^3 = 12^3 + 1^3$

Example

- There exists irrational number x and y such that x^y is rational.
- Pf.

It is known that $\sqrt{2}$ is irrational.

Now we consider the number $\sqrt{2}^{\sqrt{2}}$.

$$T \equiv \left(\sqrt{2}^{\sqrt{2}}\ is\ rational\ \vee \sqrt{2}^{\sqrt{2}}\ is\ irrational\right).$$

$Case\ 1: If \sqrt{2}^{\sqrt{2}}\ is\ rational, then\ let\ x = \sqrt{2}, and\ y = \sqrt{2}.$

$x^y = \sqrt{2}^{\sqrt{2}}$ is rational.

$Case\ 2: If \sqrt{2}^{\sqrt{2}}\ is\ irrational, then\ let\ x = \sqrt{2}^{\sqrt{2}}, and\ y = \sqrt{2}.$

$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$ is rational.

Uniqueness Proofs

- $\exists! \, xP(x) \equiv \exists x_0(P(x_0) \wedge \forall x \neq x_0 \neg P(x))$

So, we need to

1. Find an x_0 such that P(x_0) is true.
2. Show that $\wedge \, \forall x \neq x_0 \neg P(x) is \; true$

Ex. Show that if *a* and *b* are real numbers and *a* ≠0, then there is a unique real number *r* such that *ar* + *b* = 0.

Pf.

1. Let $r = -\frac{b}{a}$. We have $\text{a}\left(-\frac{b}{a}\right) + \text{b} = 0$
2. If there is a $s \neq r \; and \; as + b = 0 \, , then \; ar + b = as + b \; and \; we \; can \; get \; r = s$. This is a Contradiciton!

Open Problems and Conjectures

- An interesting property that is a believed truth but can't be proved

Theorem (Fermat's Last Theorem):

The equation $x^n + y^n = z^n$ has no solutions in integers x, y, and z with xyz $\neq$ 0 whenever n is an integer with n > 2.

Theorem (The 3x+1 Conjecture)

Let T be the transformation that sends an even integer x to x/2 and an odd integers x to 3x + 1. The 3x + 1 conjecture states that for all positive integers x, when we repeatedly apply the transform T, we will eventually reach the integer 1.

X=3, T(3) = 3x3+1 = 10, T(10) = 10/2 =5, T(5) = 3 X 5 +1 =16, T(16) = 16/2= 8, T(8) = 8/2 =4, T(4) = 4/2 = 2, T(2) = 2/2 = 1.