Logical Inference and Mathematical Proof

CSE 191, Class Note 03:
Logical Inference and Mathematical Proof
Computer Sci & Eng Dept
SUNY Buffalo

Need for inference

- Why do we study propositional and predicate logic?
  - We want to use them to solve problems.
  - To solve a problem by using logic, we often need to start from some "premises" and obtain a certain "conclusion using inference rules.
- Example: Computer scientists often need to verify the correctness of a program.
  - One possible approach is to prove the program is correct.
  - So one can start from the program and the semantics of the used programming language (i.e., the premise), and use logic inference to obtain a conclusion that the program does the right job.

What is a inference rule?

Definition:

$$\begin{array}{l} P_1 \\ P_2 \\ \hline Q \end{array}$$

is a inference rule if $(P_1 \wedge P_2) \rightarrow Q$ is a tautology.

Implication rule

The first (and simplest) rule is:

Modus Ponens (MP) Rule:

$$\begin{array}{l} P \\ P \rightarrow Q \\ \hline Q \end{array}$$

- This rule is called Modus Ponens (MP). Intuitively, if we have the condition of an implication, then we can obtain its consequence.

Example:

P	means: “there is a storm.”
$P \rightarrow Q$	means: “if there is a storm, then the office is closed.”
Q	means: “the office is closed.”

Exercise: Show $[P \wedge (P \rightarrow Q)] \rightarrow Q \equiv T$.

Another implication rule

- Recall that $P \to Q \equiv \neg P \vee Q \equiv Q \vee \neg P \equiv \neg Q \to \neg P$.
- The MP rule just studied above tells us that:

$$\begin{array}{l} \neg Q \\ \neg Q \to \neg P \\ \hline \neg P \end{array}$$

- If we replace the $\neg Q \to \neg P$ in the above with the logically equivalent proposition $P \to Q$, then we get another implication rule:

Modus Tonens (MT) Rule:

$$\begin{array}{l} \neg Q \\ P \to Q \\ \hline \neg P \end{array}$$

Exercise: Show $[\neg Q \wedge (P \to Q)] \to \neg P \equiv T$.

Logical equivalence vs. inference

By using inference rules, we can "prove" the conclusion follows from the premises. In inference, we can always replace a logic formula with another one that is logically equivalent, just as we have seen for the implication rule.

Example:

Suppose we have: $P \to (Q \to R)$ and $Q \wedge \neg R$. Use inference to show $\neg P$.

- First, we note $Q \wedge \neg R \equiv \neg(\neg Q \vee R) \equiv \neg(Q \to R)$.
- So we have the following inference:

(1)	$P \to (Q \to R)$	Premise
(2)	$Q \wedge \neg R$	Premise
(3)	$\neg(Q \to R)$	Logically equivalent to (2)
(4)	$\neg P$	Applying the second implication rule (Modus Tonens) to (1) and (3)

Yet another implication rule

Hypothetical Syllogism (HS)

$$\begin{array}{l} P \rightarrow Q \\ Q \rightarrow R \\ \hline P \rightarrow R \end{array}$$

- Intuitively, if P implies Q and Q implies R, then we can get that P implies R.

Example:

$P \rightarrow Q$	means	"if there is a storm, then the office is closed."
$Q \rightarrow R$	means	"if the office is closed, then I don't go to work."
$P \rightarrow R$	means	"if there is a storm, then I don't go to work."

Conjunction and Simplification Rules

Conjunction rule

$$\begin{array}{l} P \\ Q \\ \hline P \wedge Q \end{array}$$

Intuitively, this means when you have P and Q both being true, then $P \wedge Q$ is also true.

Simplification Rule

$$\begin{array}{l} P \wedge Q \\ \hline P \end{array}$$

Intuitively, this means when you have $P \wedge Q$ being true, clearly P is also true.

Disjunction rules

Disjunctive Syllogism (DS)

$$\begin{array}{l} P \vee Q \\ \underline{\neg P \quad\quad} \\ Q \end{array}$$

Addition Rule:

$$\begin{array}{l} \underline{P \quad\quad} \\ P \vee Q \end{array}$$

Third disjunction rule

Resolution Rule

$$\begin{array}{l} P \vee Q \\ \underline{\neg P \vee R} \\ Q \vee R \end{array}$$

- This rule plays an important role in AI systems.
- Intuitively, it means: if P implies R and $\neg P$ implies Q (why? Where do we get these implications?), then we must have either Q or R. Clearly, this is true since one of P and $\neg P$ must be true.

Other rules

We have:

$$\begin{array}{l} P \vee Q \\ P \to R \\ \underline{Q \to S} \\ R \vee S \end{array}$$

- Intuitively it means we can do inference in each of two cases (P or Q) independently.

Inference Rules

Table: Rules of Inference

Rule of Inference	Tautology	Name
p $\underline{p \to q}$ q	$(p \wedge (p \to q)) \to q$	**Modus ponens (MP)**
$\neg q$ $\underline{p \to q}$ $\neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	**Modus tonens (MT)**
$p \to q$ $\underline{q \to r}$ $p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	**Hypothetical syllogism (HS)**
$p \vee q$ $\underline{\neg p}$ q	$((p \vee q) \wedge \neg p) \to q$	**Disjunctive syllogism (DS)**
$\underline{p}$ $p \vee q$	$p \to (p \vee q)$	**Addition**
$\underline{p \wedge q}$ p	$(p \wedge q) \to p$	**Simplification**
p $\underline{q}$ $p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	**Conjunction**
$p \vee q$ $\underline{\neg p \vee r}$ $q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	**Resolution**

Valid Arguments

- A mathematical proof is always like:
  "If q_1 and $q_2 \dots$ and q_k are true, then q is true."
- The propositions $q_1, \dots, q_k$ are called the premises.
- The proposition q is called the conclusion.
- The mathematical proof is really to show that $(q_1 \wedge q_2 \dots \wedge q_k) \rightarrow q$ is a tautology.

To do this, we can either:

- Directly prove $(q_1 \wedge q_2 \dots \wedge q_k) \rightarrow q \equiv T$ by using logic equivalence rules, (which will be very long); or
- Present a valid argument, by using logic inference rules, defined in the following slide.

How to build a valid argument?

A valid argument is a sequence of propositions $P_1, P_2, \dots, P_n$ such that:

- P_n is the conclusion q.
- Each P_i $(1 \le i \le n)$ is:
  - either a premise (namely some q_j);
  - or a proposition that can be obtained from previous propositions by using a rule of inference;
  - or a proposition that is logically equivalent to a previous proposition.
  - Or a tautology.

Remark:

If $P_1, P_2, \dots, P_n, Q$ is a valid argument, then we can always show:

$$[q_1 \wedge q_2 \wedge \cdots \wedge q_k] \rightarrow q \equiv T \tag{1}$$

by using logic equivalence rules.
So a valid argument is just a shorter way to prove (1) is a tautology by using logic equivalence rules.

Inference example

Consider the following propositions:
p: It's sunny this afternoon.
q: It's colder than yesterday.
r: We will go swimming.
s: We will take a canoe trip.
t: We will be home by sunset.

Example:

Premises:

a. "It's not sunny and it's colder than yesterday" $\neg p \land q$
b. "We will go swimming only if it's sunny." $r \to p$
c. "If we don't go swimming then we will take canoe trip." $\neg r \to s$
d. "If we take a canoe trip, then we will be home by sunset." $s \to t$

Conclusion: "We will be home by sunset." t.

Inference example

(1)	$\neg p \land q$	Premise
(2)	$\neg p$	Simplification rule using (1)
(3)	$r \to p$	Premise
(4)	$\neg r$	MT using (2) (3)
(5)	$\neg r \to s$	Premise
(6)	s	MP using (4) (5)
(7)	$s \to t$	Premise
(8)	t	MP using (6) (7)

This is a valid argument showing that from the premises (a), (b), (c) and (d), we can prove the conclusion t.

Inference example

Example:

Suppose $P \to Q$; $\neg P \to R$; $Q \to S$. Prove that $\neg R \to S$.

(1)	$P \to Q$	Premise
(2)	$\neg P \vee Q$	Logically equivalent to (1)
(3)	$\neg P \to R$	Premise
(4)	$P \vee R$	Logically equivalent to (3)
(5)	$Q \vee R$	Apply resolution rule to (2)(4)
(6)	$\neg R \to Q$	Logically equivalent to (5)
(7)	$Q \to S$	Premise
(8)	$\neg R \to S$	Apply HS rule to (6)(7)

A more concrete example

Example: Suppose:

(1) If it is Saturday today, then we play soccer or basketball.
(2) If the soccer field is occupied, we dont play soccer.
(3) It is Saturday today, and the soccer field is occupied.
Prove: “we play basketball or volleyball”.

First we formalize the problem:
P: It is Saturday today.
Q: We play soccer.
R: We play basketball.
S: The soccer field is occupied.
T: We play volleyball.
Premise: $P \to (Q \vee R),\ S \to \neg Q,\ P,\ S$
Need to prove: $R \vee T$.

A more concrete example

(1)	$P \rightarrow (Q \vee R)$	Premise
(2)	P	Premise
(3)	$Q \vee R$	Apply MP rule to (1)(2)
(4)	$S \rightarrow \neg Q$	Premise
(5)	S	Premise
(6)	$\neg Q$	Apply MP rule to (4)(5)
(7)	R	Apply DS rule to (3)(6)
(8)	$R \vee T$	Apply Addition rule to (7)

Solving a murder case

The following is a murder case solved by Sherlock Holmes, in “A Study in Scarlet” (a detective mystery novel by Sir Arthur Conan Doyle).

Quote from “A Study in Scarlet”

> *“And now we come to the great question as to the reason why. Robbery has not been the object of the murder, for nothing was taken. Was it politics, then, or was it a woman? That is the question which confronted me. I was inclined from the first to the latter supposition. Political assassins are only too glad to do their work and fly. This murder had, on the contrary, been done most deliberately, and the perpetrator has left his tracks all over the room, showing he had been there all the time.”*

From these, Sherlock Holmes concluded: “It was a woman”.

Solving a murder case

Known premises:

1. If it’s a robbery, something would have been taken.
2. Nothing was taken.
3. If it’s not a robbery, it must be politics or a woman.
4. It it’s politics, the assassin would have left immediately.
5. If assassin left tracks all over the room, he cannot have left immediately.
6. The assassin left tracks all over the room.

Show the conclusion: “It was a woman”.
We will discuss this example in class.

Inference with quantifiers

Many inferences in Math and CS involve quantifiers.

Example 1:

- All computer science majors must take CSE 191.
- CSE 191 students study discrete structures.
- So, all computer science majors must study discrete structures.

Example 2: The definition of limit in Calculus:

$\lim_{x\to a} f(x) = b$ if and only if

$$\forall\, \epsilon > 0\; \exists\, \delta > 0\; \forall\, x\; (|x-a| \le \delta) \to (|f(x)-b| < \epsilon)$$

Question:

How do you show $\lim_{x\to a} f(x) \neq b$?

Universal quantification rules

Consider the following two formulas:

- $\forall\, xP(x)$.
- $P(c)$ for an arbitrary c.

Starting from either of them we can obtain the other.

Example:

- Everybody has a nose.
- C has a nose (where C can be anybody).

Universal quantification rules

Universal instantiation rule:

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

Universal generalization rule:

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

Existential quantification rules

Consider the following two formulas:

- $\exists\, x\; P(x)$.
- $P(c)$ for some c.

Starting from either of them we can obtain the other.

Example:

- There is a student living in Amherst.
- John lives in Amherst.

Existential quantification rules

Existential instantiation rule:

$$\frac{\exists\, x\; P(x)}{P(c) \text{ for some } c}$$

Existential generalization rule:

$$\frac{P(c) \text{ for some } c}{\exists\, x\; P(x)}$$

Rules of Inference for Quantified Statements

Table: Rules of Inference for Quantified Statements

Rule of Inference	Name
$\dfrac{\forall x P(x)}{p(c) \text{ for an arbitrary element } c}$	Universal Instantiation
$\dfrac{P(c) \text{ for an arbitrary element } c}{\forall x P(x)}$	Universal generalization
$\dfrac{\exists x P(x)}{p(c) \text{ for some element } c}$	Existential Instantiation
$\dfrac{P(c) \text{ for some element } c}{\exists x P(x)}$	Existential generalization

Inference example

Example:

Premises:

1. “A student in this class has not read the book”.
2. “Everyone in this class passed the first exam”.

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 has passed the first exam”.

Then:

1. $\exists x(C(x) \wedge \neg B(x))$.
2. $\forall x(C(x) \rightarrow P(x))$.

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

We will show the inference in class.

An arithmetic example

Example: Suppose:

- all natural numbers are integers;
- there exists a natural number;

Prove that there exists an integer.

We can formalize this problem as follows. (Let the universe of discourse be all real numbers.)

$N(x)$: x is a natural number.
$I(x)$: x is an integer.
Premise: $\forall\, x\ (N(x) \to I(x)),\ \exists\, x\, N(x)$
Need to prove: $\exists\, x\, I(x)$

An arithmetic example

(1)	$\exists\, x\, N(x)$	Premise
(2)	$N(c)$	Apply existential instantiation rule to (1)
(3)	$\forall\, x\ (N(x) \to I(x))$	Premise
(4)	$N(c) \to I(c)$	Apply universal instantiation rule to (3)
(5)	$I(c)$	Apply MP rule to (2)(4)
(6)	$\exists\, x\, I(x)$	Apply existential generalization rule to (5)

From Inference to Proof

- In fact, the process of logical inference is also the process of giving a formal proof.
- In mathematics, we need to do a lot of proofs.
  - However, formal proofs are too long, since in each step we can only apply a simple inference rule.
  - Formal proofs are also too hard to follow since we can be easily buried in details and thus miss bigger pictures.

(Informal) mathematical proof

A mathematical proof is usually “informal”. (Compared to logical inferences we just studied. But still much more formal than everyday language.)

- More than one rule may be used in a step.
- Steps may be skipped.
- Axioms may be assumed.
- Rules for inference may not be explicitly stated.

Some terminology

- Theorem: statement that can be shown true.
  - Proposition: less important theorem.
  - Lemma: less important theorem used to prove other theorems.
  - Corollary: theorem that trivially follows another theorem.
- Conjecture: statement that is proposed to be true, but has not been proved.
- Axiom: statement assumed to be true (i.e., true statement that does not need a proof).

Convention on universal quantifier

- Many mathematical theorems are about a property of elements in a domain, and hence need universal quantifiers.
- However, many such universal quantifiers are omitted.

Example:

If $a > b$, then $a - b > 0$.

- This actually means, for all real numbers a and b, if $a > b$, then $a - b > 0$.

Proof method: direct proof

Definition

A direct proof for $p \to q$ starts by assuming p and finishes by establishing q.

- In the proof, we can use axioms, previously proven theorems, and inference rules.

Example of direct proof:

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

Proof: Since n is an odd integer, there exists integer k such that $n = 2k + 1$. Hence:
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1$.
Since k is an integer, $2k^2 + 2k$ is also an integer. So $2 \cdot (2k^2 + 2k)$ is even. Therefore, n^2 is an odd integer.

Proof by contraposition

- Another method for proof is proof by contraposition.
- Note that $p \to q$ is logically equivalent to $\neg q \to \neg p$.

Definition

A proof by contraposition for $p \to q$ is actually a direct proof for $\neg q \to \neg p$.

- It starts by assuming $\neg q$, and finishes by establishing $\neg p$.
- In the proof, we can also use axioms, previously proven theorems, and inference rules.

Example for proof by contraposition

Example:

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

Proof: We prove it by contraposition. Suppose n is not odd. Then it is even.
So there exists an integer k such that $n = 2k$.
Hence: $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.
Since k is an integer, $3k + 1$ is also an integer. Therefore, $3n + 2$ is even, i.e., $3n + 2$ is not odd.

Proof by contradiction

- Yet another method for proof is proof by contradiction.
- Note that p is logically equivalent to $\neg p \rightarrow (r \wedge \neg r)$.

Definition

A proof by contradiction for p is actually a direct proof for $\neg p \rightarrow (r \wedge \neg r)$.

- It starts by assuming $\neg p$ and finishes by establishing both r and $\neg r$.
- In the proof, we can also use axioms, previously proven theorems, and inference rules.

Example for proof by contradiction (1)

Example:

Prove that there is no positive integer n such that $n^3 + 1 = 100$.

Proof: We prove it by contradiction.
Suppose that there is a positive integer n such that $n^3 + 1 = 100$.
If $n \leq 4$, then $n^3 + 1 \leq 4^3 + 1 = 65 < 100$. Impossible.
If $n \geq 5$, then $n^3 + 1 \geq 5^3 + 1 = 126 > 100$. Still impossible.
Contradiction.

Example for proof by contradiction (2)

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

Proof (Hinted by Aristotle, 384-322 BC): We prove it by contradiction.

- Suppose that $r = \sqrt{2}$ is a rational number. Then there exist integers a and b such that $r = a/b$.
- Further, we assume that a and b have no common divisors. (If they have common divisors, divide both a and b by their greatest common divisors.)
- Hence, $2 = r^2 = (a/b)^2 = a^2/b^2$.
- So we get that $a^2 = 2 \cdot b^2$, which is an even number.
- Therefore, a is even. Thus, there exists integer c such that $a = 2c$.
- This implies that $(2c)^2 = a^2 = 2 \cdot b^2$, i.e., $2c^2 = b^2$.
- Hence, b^2 is even, which means b is also even.
- Since a and b are both even, they have a common divisor 2. Contradiction.

Example for proof by contradiction (3)

Definition

A prime number is a positive integer whose only divisors are 1 and itself.

- The first few prime numbers: 2, 3, 5, 7, 11, 13, 17 ...
- At the beginning, the prime numbers are dense (i.e. there are many of them). For example, there are 168 prime numbers between 1 and 1000.
- When the number gets bigger, the prime numbers are sparse (i.e. there are few of them).
- How many prime numbers are there? Finite? or infinite?

Theorem:

There are infinitely many prime numbers.

Example for proof by contradiction (3)

Proof: (Euclid 325 -265 BC).

We prove this by contradiction. Assume there are only finitely many primes: $p_1, p_2, \ldots, p_n$. Consider the number $Q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

- We ask: Is Q a prime number?
- Because $Q > p_i$ for all $1 \leq i \leq n$ and $p_1, \ldots, p_n$ are ALL prime numbers, Q IS NOT a prime.
- If Q is not a prime, it must have a prime factor.
  - So one of p_i $(1 \leq i \leq n)$ must be a factor of Q.
  - But Q divided by each p_i has remainder 1.
  - So none of p_i $(1 \leq i \leq n)$ is a divisor of Q. Hence Q IS a prime.
- A contradiction.

- It is the first proof in the book “Proofs from THE BOOK”, where THE BOOK refers to the imagined collection of the most elegant proofs that the famous mathematician Paul Erdös claimed is maintained by the God.

Proof by cases

- Note that $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$ is logically equivalent to $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)$.

Definition:

A proof by cases for $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$ is actually a direct proof for $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)$.

- First, it lists n cases. In the ith case, it starts by assuming p_i and finishes by establishing q.
- In the proof, we can also use axioms, previously proven theorems, and inference rules.

Example for proof by cases (1)

Example:

Prove that $n + 100 > 3^n$ if n is a positive integer with $1 \leq n \leq 3$.

Proof: We prove it by cases.
Case 1: $n = 1$. Then, $n + 100 = 101 > 3 = 3^n$.
Case 2: $n = 2$. Then, $n + 100 = 102 > 9 = 3^n$.
Case 3: $n = 3$. Then, $n + 100 = 103 > 27 = 3^n$.

Example for proof by cases (2)

Example:

Prove that if n is an integer, then $n^2 \geq n$.

Proof: We prove it by cases.
Case 1: $n = 0$. Then, $n^2 = 0 = n$.
Case 2: $n \geq 1$. Then, $n > 0$. So we can multiply both sides of inequality by n, and get $n^2 \geq n$.
Case 3: $n \leq -1$. Hence, $n^2 \geq 0 > -1 \geq n$.

Notion of Without Loss of Generality

- In some "proof by cases", there are too many cases.
- Some of the cases are similar to each other.
- To shorten the proof, we only give detailed proofs of some cases, but omit the proof of other cases.
- When we do this, we say Without Loss of Generality (often abbreviated as WLOG).

Example of Without Loss of Generality

Example:

Prove that if x and y are integers and both $x + y$ and $x \cdot y$ are even, then both x and y are even.

Proof: We will use: proof by contraposition, the notion of WLOG, and proof by cases.
First suppose that x and y are not both even. That is we assume either x is odd, or y is odd (or both).
WLOG, we assume x is odd.
Case 1: y is even. Then $x + y =$ odd + even = odd. This contradicts the assumption that $x + y$ is even.
Case 2: y is odd. Then $x \cdot y =$ odd $\cdot$ odd = odd. This contradicts the assumption that $x \cdot y$ is even.
In both cases, we get a contradiction. Hence both x and y must be even.

Example of Without Loss of Generality

- In this example, when we say WLOG, we are saying the other case (that y is odd) can be proved by using similar method.
- When using WLOG, you must make sure the omitted cases are really similar to the proved cases.
- Otherwise, your proof is incomplete and could be wrong.

Constructive proof

- Note that $\exists\, x\ P(x)$ is equivalent to "$P(c)$ is true for some c".

Definition

A constructive proof for $\exists\, x\ P(x)$ finds c such that $P(c)$ is true. Hence, we can conclude that $\exists\, x\ P(x)$ is also true.

Example:

Prove that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Proof: We construct an example for such a positive integer:

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

Non-constructive proof

- To prove $\exists\, x\ P(x)$, we can just provide a specific c such that $P(c)$ is true.
- But sometimes we cannot do this.
- It is still possible to argue such element exists, even though we cannot pin point the specific c.
- This is called non-constructive proof.

Non-Constructive proof example

Example:

Prove that there exist irrational numbers a and b such that a^b is rational.

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

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational. Then let $a = \sqrt{2}$ and $b = \sqrt{2}$. Then a^b is rational.

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is not rational. Then let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$.
Then $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ is rational.

- Note that, in this proof, we do not claim/know if $\sqrt{2}^{\sqrt{2}}$ is a rational number or not.
- But in either case, we prove the proposition.
- Actually, $\sqrt{2}^{\sqrt{2}}$ is irrational. But the proof requires high powered mathematical theory, far beyond our reach.

Uniqueness proof

- In mathematics we often need to prove there exists a unique x such that $P(x)$ is true.
- We often prove the following two things (which, when combined together, are logically equivalent to the original statement):
  - There exists x such that $P(x)$ is true. (Namely $\exists\, x\, P(x)$).
  - If $P(x)$ and $P(y)$ are both true, then $x = y$. (Namely $\forall\, x\, \forall\, y\, (P(x) \wedge P(y)) \rightarrow (x = y)$.

In some books, we use the symbol $\exists!$ for “there exists a unique ....”.

Example for uniqueness proof

Example:

Prove that if a and b are real numbers and a is not 0, then there is a unique real number r such that $ar + b = 0$.
(In other words: There is a unique solution for the equation $ax + b = 0$.

Proof:

- First, we show that there exists such an r. Let $r = -b/a$. Then:

  $$ar + b = a(-b/a) + b = -b + b = 0$$

  So this r satisfies the condition.
- Second, suppose that r and r' both satisfy the condition. Then, $r - r' = ((ar + b) - (ar' + b))/a = (0 - 0)/a = 0$, which implies that $r = r'$.

Logic Dilemmas

Definition

A statement p is a dilemma if we cannot prove $p \equiv$ T nor $p \equiv$ F.

Example: Barber's dilemma

Premise: "The barber gives haircut to a person if and only if that person doesn't give haircut to himself".
Statement p: "The barber gives haircut to himself."
Question: Is p true or false?

- If p is true: Then the premises states that he does not give haircut to himself. This implies p is false.
- If p is false: Then the premises states that he does give haircut to himself. This implies p is true.
- So we cannot say if p is true or false. And the statement is a dilemma.

Gödel's Incompleteness Theorem.

Definition:

A "logic inference system" consists of a collection of "rules of inferences" and a collection of "axioms".

Definition:

A logic inference" system is "consistent" if for any proposition p, we can prove either $p \equiv$ T, or $p \equiv$ F, (or neither), but not both.

- An inconsistent logic inference system is useless, because we can "prove" $p \equiv$ T for any proposition p in such a system.

Definition:

A logic inference system is "complete" if for any proposition p, we can prove either $p \equiv$ T or $p \equiv$ F, (or both).

- The logic inference system we have studied is incomplete because there are propositions that we cannot prove to be T or F.

Gödel's Incompleteness Theorem.

Question:

- It is unsettling that our logic inference system (the foundation of all mathematics, computer science ....) is INCOMPLETE.
- Can we make it "stronger" by adding a few new "rules of inferences"?
- If these new rules can be derived from existing rules, we don't gain anything.
- If the new rules are too "strong", they will make our inference system "inconsistent".
- It would be ideal if we have a logic inference system that is both consistent and complete.
- Can this be done?

Gödel's Incompleteness Theorem.

Unfortunately:

Gödel's Incompleteness Theorem (1931)

Any consistent logic inference system MUST BE incomplete.

Hilbert's Problems

- In 1900, David Hilbert (one of the greatest mathematician of his time) presented 23 unsolved problems to the mathematicians of the 20th century.
- All these problems are extremely hard.
- Some of Hilbert's problems have been solved (either positively or negatively). Some are not.

Hilbert's Second Problem:

Prove that "The logic inference system for arithmetic is complete".

- Gödel's Incompleteness Theorem is the negative answer to Hilbert's Second problem.
- We will mention Hilbert's first problem later (which remains unsolved).

Hilbert's Second Problem

What is Hilbert 2nd problem really asking?

Axioms of Arithmetic

Basic objects: The set of natural numbers: 1, 2, 3, 4 . . .
Operations: $+, -, \times, \div$
Axioms:

- if $a = b$ then $b = a$. i.e $\forall a \forall b (a = b) \rightarrow (b = a)$.
- if $a = b$ and $b = c$ then $a = c$ i.e $\forall a \forall b \forall c (a = b) \wedge (b = c) \rightarrow (a = c)$.
- $a + 0 = a$ i.e $\forall a (a + 0 = a)$.
- $a + b = b + a$ i.e $\forall a \forall b (a + b = b + a)$.
- $(a + b) + c = a + (b + c)$ i.e $\forall a \forall b \forall c (a + b) + c = a + (b + c)$.

  $\vdots$

  plus all basic arithmetic laws you learned before the third grade.

These axioms plus our table of inference rules constitute ”the logic inference system for arithmetic”.

Logic Inference System for Arithmetic

- This inference system looks really elementary (after all, you learned everything in it before the 3rd grade!)
- There cannot be hard problems in this system, right?
- Completely wrong!

Some hard arithmetic problems

- There are many integer solutions for the equation: $x^2 + y^2 = z^2$.
- For examples: $3^2 + 4^2 = 5^2,\ 5^2 + 12^2 = 13^2 \ldots$
- Are there positive integer solutions for the equation: $x^3 + y^3 = z^3$?

Fermat's Last Theorem:

For any integer $n \geq 3$, there is no positive integer solution x, y, z for the equation

$$x^n + y^n = z^n$$

Equivalently, we want to show the following proposition is T (the domain for n, x, y, z is all positive integers.)

$$\forall (n \geq 3) \neg \exists x\ \exists y\ \exists z\ (x^n + y^n = z^n)$$

This problem had been open for more than 350 years. It was proved by Andrew Wildes (a Math professor at Princeton University) in 1995.

Some hard arithmetic problems

Goldbach's Conjecture:

Every even integer $n \geq 2$ is the sum of two prime numbers.

Example: 4=2+2; 6=3+3; 8=3+5; . . ., 20=3+17; 22 = 3+19= 11+11; . . ..

- Let $E(x)$ be the proposition x is even; $P(y)$ be the proposition y is a prime number. Then Goldbach's Conjecture is to prove the following proposition is T:

$$\forall x (E(x) \rightarrow (\exists y\ \exists z\ (P(y) \wedge P(z) \wedge (x = y + z)))$$

- It has been verified that this conjecture is true for n up to $1.6 \cdot 10^{18}$.
- British publisher Tony Faber offered a \$1,000,000 prize if a proof was submitted before April 2002. The prize was not claimed.
- It remains unsolved today.

Hilbert's 2nd Problem

- Hilbert imagined that all propositions (involving only integers and arithmetic operations) can be proved either T or F.
- These propositions would include the propositions for Fermat's Last Theorem and Goldbach's Conjecture (and many other unsolved hard problems).
- Gödel's Incompleteness Theorem says: "this is a mission impossible!"