Week 5: Proof

Tommy WS Chow

EE

CityU

Sept 2020

Important Symbols

- $P \rightarrow Q$ *:* If P, then Q
- $P \Leftrightarrow Q$ *:* P if and only if Q
- $x \in S$ *:* x belongs to S, x *is an element/member of* S
- $S \subseteq T$*:* S is a subset of T, or S is *contained* in T
- $\forall x$: for all x
- $\exists x$*:* there exists x
- P **AND** Q : the **conjunction** of P and Q
- P **OR** Q : the **disjunction** of P and Q
- $\sim P$: Not P

Logic and Proof

- Logic is the study of correct reasoning.
  - Definition: a **statement** or **proposition** is a sentence that is either TRUE or False.
  - Example: The year 2000 is a leap year.

    $3 + 2 = 6.\ \pi^2 < 10.$

    The decimal expression of π contains one hundred consecutive 3's.

  However, the following sentences are not statements:

    Let $x = 4$.

    Find the nearest integer to $\sqrt{5}^{13}$.

    Is it Friday today?

Basic Logic

- Propositional logic: the part of logic that deals with combining statements using connectives such as AND, OR, NOT, or implies.
  - Definition: Let P and Q be statements.
    - The statement P **AND** Q is called the **conjunction** of P and Q. The statement P AND Q will be TRUE if P is TRUE and Q is TRUE but will be FALSE otherwise.
    - The statement P **OR** Q is called the **disjunction** of P and Q. The statement P OR Q will be TRUE if P is TRUE or Q is TRUE, or both are TRUE.
    - The **negation** of the statement P is denoted by **NOT** P. Another very common notation is $\sim P$.

NOT

x	x'
0	1
1	0

AND

x	y	xy
0	0	0
0	1	0
1	0	0
1	1	1

OR

x	y	$x+y$
0	0	0
0	1	1
1	0	1
1	1	1

Propositional Logic

- The basic building block of logic – **propositions**
- A **proposition** is a declarative sentence that is either true or false, but not both.

Example:

1. Washington D.C is the capital of USA
2. Toronto is the capital of Canada
3. 1+2=3
4. 2+2=3

Propositions 1 and 3 are true, whereas 2 and 4 are false

Negation of propositions

Find the negation of the proposition "Today is Friday" and express in simple English

"It is not the case that today is Friday" or simple language "Today is not Friday"

Conditional Statement $P \Longrightarrow Q$

- In mathematics, we often use statements of the form "If P, then Q". This is called a **conditional statement** or **implication**, where P is the *hypothesis* and Q is the *conclusion*.
  - Definition: given two statements of P and Q, the **conditional statement** "If P, then Q" is denoted by $P \Longrightarrow Q$ and is defined by the following truth table.

P	Q	$P \Longrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

"If 5 <7, then 2+2 =3" is a true statement.

If and only If

- Definition: given two statements P and Q, we denote the statement "***P* if and only if *Q***" by $P \Leftrightarrow Q$, and define it by $(P \Longrightarrow Q)$ AND $(Q \Longrightarrow P)$. The truth table is given below.

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

- The statement $P \Leftrightarrow Q$ is true precisely when P and Q have the same truth values.

Example: Let p be the statement "You can take the flight", and q be "You buy a ticket"   Then $P \Leftrightarrow Q$ is the statement
"You can take the flight if and only if you buy a ticket."

Examples

Let *P* be the statement "*I can walk*", *Q* be the statement "*I have broken my leg*" and *R* be "*I take the bus*". Express the below statement in English sentence.

1. $Q \Longrightarrow \text{NOT } P,$ 2. $P \Leftrightarrow NOT\ Q$

Solutions:

1. If I have broken my leg then I cannot walk
2. I can walk if and only if I have not broken my leg

Class Exercises: write the bellows it in simple language.

1. $R \Longrightarrow (\text{Q OR NOT } P)$ 2. $R \Longrightarrow (\text{Q} \Leftrightarrow \text{NOT } P)$

Example: Divisibility

The ***divisibility*** relation $a|b$ can be defined symbolically as

$\exists q, \quad b = qa$, read as a divides b,

$\text{i.e.,} \;\; 20 = (10)(2), 20 = \text{b}, \text{q} = 10, \text{a} = 2,$ so read 2 divides 20.

where the universe of discourse is the set of integers.

Is 2|12 true or false? Yes, it is true.

Using this definition, determine whether (i) 0|3 and (ii) 0|0 is true or false.

Solution.

(i) 0|3 is equivalent to $\exists q$, 3= q0;

that is, $\exists q$, 3=0.

Since 3=0 is always false,

0|3 is False.

(ii) 0|0 is equivalent to $\exists q$, 0= q0; that is, $\exists q$, 0=0.

Since 0=0 is always true,

we can choose q as any integer, and so 0|0 is true.

Quantifier Negation Rules

$$\text{NOT}\left(\forall x,\ P(x)\right) \text{ is equivalent to } (\exists x, \text{NOT } P(x)).$$

$$\text{NOT}\left(\exists x,\ P(x)\right) \text{ is equivalent to } (\forall x, \text{NOT } P(x)).$$

In general, two statements involving quantifiers will be *equivalent* if they have the same meaning.

We cannot always use truth tables to check for equivalence or implications involving quantifiers.

So at this stage we have to reason informally to check the equivalence or implication.

Example:

Universe of discourse is the set of integers that are assumed to lie in a particular set. what does the following statement mean in English? How to prove it true for false?

$$\exists x \; \forall y \in Z, (\mathrm{x} \geq y).$$

Solution. The statement is "There is an integer that is greater than or equal to all integers." In simple language, it means that there is a largest integer.

The statement is false.

Show it is false, we need to prove $x, y \in Z$,

$$\mathrm{NOT}(\exists x \; \forall y, (\mathrm{x} \geq y)) \text{ is true}.$$

This is equivalent to the following statements.

$$\forall x, \mathrm{NOT}\big(\forall y, (\mathrm{x} \geq y)\big).$$

$$\forall x \; \exists y, \mathrm{NOT}(\mathrm{x} \geq y).$$

$$\forall x \; \exists y, (\mathrm{x} < y).$$

The last statement is true because, for every x, we can take $y = x + 1$.

Proofs

Many mathematical theorems can expressed symbolically in the form

$$P \Longrightarrow Q.$$

The statement P: the assumption or hypothesis

The statement Q: the conclusion.

- Ways to prove a result:
  - Understand the definitions.
  - Try examples.
  - Try standard proof methods.

Types of Proof

- Direct Proof
- If and only If proof: Proving $P \Leftrightarrow Q$, "*if and only if*" or the phrase "*necessity and sufficiency*."
- Contrapositive proof: prove $P \Longrightarrow Q$ is equivalent to prove NOT $Q \Longrightarrow$ NOT P

- Proof by counterexample
- Proof by Contradiction
- Mathematical Induction

Example 1: Direct Proof Method

- Proving $P \Longrightarrow Q$ (conditional statement)

The direct method of proving $P \Longrightarrow Q$ is to assume that the hypothesis P is true, and use this to prove that the conclusion Q is true.

- **Proposition.** If $S \cap T = S$, then $S \subseteq T$.

Proof. Suppose that $S \cap T = S$. To prove that S is a subset of T, we need to prove that if $x \in S$, then $x \in T$.

Let $x \in S$, so that $x \in S \cap T$, since $S \cap T = S$. It follows from the definition of the intersection of sets that $x \in T$. It now follows from the definition of inclusion that $S \subseteq T$.

Example 2: Direct proof

Prove $A \subseteq B \; and \; C \subseteq D \Longrightarrow (A \; X \; C) \subseteq (B \; X \; D)$
Recall Cartesian product definition $A \; X \; C$ =$\{(x, y) \mid x \in A \;\&\; y \in B\}$

Approach of thinking: We start from the given, suppose $A \subseteq B \; and \; C \subseteq D$, we need to show $A \; X \; C$ is contained in $B \; X \; D$, or every element of $A \; X \; C$ is in the set B X D.

Proof: Take any arbitrary element $(x, y) \in A \; X \; C$, which means $x \in A$, & $y \in C$
since $x \in A$ & $A \subseteq B$, then $x \in B$,
since $y \in C$ & $C \subseteq D$, then $y \in D$,
thus $(x, y) \in B \; X \; D$.
This shows $(A \; X \; C) \subseteq (B \; X \; D)$. *Proved.*

Example 3: Direct proof

Let $a, b \in R$. Prove that if $a < b < 0$, $a^2 > b^2$.

PROOF: Let $a, b \in R$, and assume that $a < b < 0$.
Important that a, b are real numbers (means not imaginary number, *i*)

Obviously the above $A = \pi r^2 \Longrightarrow$ $a < 0$, or a and b are negative.
As we want to prove $a^2 > b^2$, so we start from multiple the given

$a < b$ by a, $(a)(a) > (a)(b)$ (inequality change sign because a is negative)

$\Longrightarrow$ $a^2 > ab$ (a).

But given $a < b$ (initial given condition), multiple it by b.
We have $ab > bb > b^2$, substitute it back to (a).

We have $a^2 > b^2$. Proved.

If and only If Proof

- Proving $P \Leftrightarrow Q$ This is the "*if and only if*" or the phrase "*necessity and sufficiency*."

  "P if and only if Q" can be split up into the **two steps**,

  1. the "only if" part $P \Longrightarrow Q$ *(*sufficiency*)*, and

  2. the "if" part $Q \Longrightarrow P$ (necessity). Each step is usually proved separately.

Example: If I study hard, then I pass.

AND If I pass then I studied hard.

Combine them: "I will pass if and only if I study hard."

Example 1: If and Only If Proof

Let p and q be real numbers
Let $\boldsymbol{E}$ denote the equation $x^2 + px + q = 0$
Prove that E has 2 distinct solutions Iff $p^2 - 4q > 0$

As it is iff, we use 2 steps to prove it.

i) Prove if $p^2 - 4q > 0$, then E has 2 distinct solutions.

By quadratic formula, the 2 solutions are $\frac{-p+\sqrt{p^2-4q}}{2}$ and $\frac{-p-\sqrt{p^2-4q}}{2}$

since $p^2 - 4q > 0$, $\sqrt{p^2 - 4q}$ is real and positive, thus the above 2 solutions are distinct and Real.

ii) Prove the other direction. Prove if E has 2 distinct solutions, then $p^2 - 4q > 0$

Suppose that E has 2 distinct Real solutions α and β, $\alpha \neq \beta$, then we can write

$x^2 + px + q = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$

Comparing coefficient: $p = -(\alpha + \beta)$, $q = \alpha\beta$

Thus $p^2 - 4q = (-(\alpha + \beta))^2 - 4\alpha\beta = \alpha^2 + \beta^2 + 2\alpha\beta - 4\alpha\beta = \alpha^2 + \beta^2 - 2\alpha\beta$

$p^2 - 4q = (\alpha - \beta)^2$. As $\alpha \neq \beta$ and Real, $(\alpha - \beta)^2 > 0$

Thus, $p^2 - 4q > 0$ proved.

Thus, E has 2 distinct solutions Iff $p^2 - 4q > 0$

Example 2: If and only If proof

"P if and only if Q" split up into the **two steps**,

1. the "only if" part $P \Longrightarrow Q$ *(*sufficiency*)*, and
2. the "if" part $Q \Longrightarrow P$ (necessity).

- **Proposition.** If $S \cap T = S \cup T$, if and only if $S = T$.

Proof*.* *1.* To prove $(S \cap T = S \cup T) \Longrightarrow (S = T)$,

suppose $S \cap T = S \cup T$. If $x \in S$ then $x \in S \cup T$.

Since $S \cap T = S \cup T$, $x \in S \cap T$, and hence $x \in T$. This proves that $S \subseteq T$.

This problem is symmetric in S and T, since interchanging S and T leaves the problem unchanged.

Hence a similar proof, which S and T interchanged, will show that $T \subseteq S$. Combing $S \subseteq T$ with $T \subseteq S$ shows that $S = T$.

2. The other direction of $(S = T) \Longrightarrow (S \cap T = S \cup T)$ is straightforward. Suppose that S=T. Then $S \cap T = S \cap S = S$

and $S \cup T = S \cup S = S$, so $S \cap T = S \cup T$.

Example: Contrapositive

The contrapositive of the general implication *“**If P then Q**”* is the statement *“If **not Q**, then **not P**”*

For example “If it rains then I get wet” is the statement “If I am not wet, then it is not raining

$P \Longrightarrow Q$ is equivalent to NOT $Q \Longrightarrow$ NOT P
We use a truth table to prove

P	Q	$P \Rightarrow Q$	NOT Q	NOT P	NOT $Q \Rightarrow$ NOT P
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

We see from the truth table that $P \Longrightarrow Q$ is equivalent to NOT $Q \Longrightarrow$ NOT P

Example 2: Proof by Contrapositive

- Proving $P \Longrightarrow Q$

In this method, we prove the statement $P \Longrightarrow Q$ by proving its contrapositive NOT $Q \Longrightarrow$ NOT P.

- **Proposition.** If x is a real number such that $x^3 + 7x^2 < 9$, then $x < 1.1$.

Proof. The contrapositive of the statement that

"If $x \geq 1.1$, then $x^3 + 7x^2 \geq 9$." So we prove this.

Suppose that $x \geq 1.1$. In particular, x is positive, and so

$$x^3 + 7x^2 \geq 1.1^3 + 7(1.1)^2 = 1.331 + 8.47 = 9.801 \geq 9.$$

Therefore, by the Contrapositive Proof Method, the original result must be true.

Class Work: contrapositive proof

$N \in Z$, use contrapositive proof to prove if n^2 is even, then n is even.

Contrapositive: step 1 to flip the statement and becomes If n is NOT even, then n^2 is NOT even.

Proof by Counterexamples

Sometimes a conjectured result in mathematics is not true. In that case, we would not be able to prove it.

However, we could try to disprove it -- try to prove that negation is true.

If the statement (conjecture) is of the form

$$\forall x, P(x),$$

then its negation is NOT $(\forall x, P(x))$, which is equivalent to

$$\exists x, \text{NOT } P(x).$$

- To disprove the statement $\forall x, P(x)$ we only have to find *one value* of x, say c, such that $P(c)$ is false.
- This c is called a **counterexample** to the statement $\forall x, P(x)$.

Example 1: Proof by Counterexample

Let x be a real number. Disprove the statement

$$\text{If } x^2 > 9 \text{ then, } x > 3.$$

Solution. One counterexample to the statement is obtained by taking $x = c = -4$,

since $c^2 = 16 > 9$ and $c \leq 3$.

This counterexample disproves the statement.

Example: Proof by Counterexample

Let m and n be integers. If m or n is odd, is it necessarily true that $m^3 + n^3$ is odd?

Solution. The answer to the question is **NO**, since we can easily find a counter example in which m or n is odd, and $m^3 + n^3$ is even.

One such counterexample is $m = 1$ and $n = 1$.

Notice that the mathematical inclusive OR is necessary here. Of course, there is an infinite number of counterexamples in this case; they occur when m and n are both odd. However, **one counterexample is enough to disprove the result.**

Class work: Counterexamples

Give a counterexample to the below

1. "If n is an integer and n is divisible by 4, then n^2 is divisible by 4"

Proof by Contradiction

Proof technique called proof by contradiction assume that the statement we want to prove is false and then show that this implies a contradiction.

- For example, suppose we wanted to prove the statement Q. If we can show that NOT Q leads to a contradiction, then NOT Q must be false; that is, Q must be true.

- **Proposition.** There is no largest integer.

Proof. We assume a NOT Q first that is suppose there is a largest integer, which is n . We know $n + 1$ is also an integer. And n+1 is larger than than n.

This **contradicts** our assumption that n was the largest integer. Hence there is no largest integer.

Example 1: Proof by Contradiction

- **Proposition.** There is no real solution to $x^2 - 6x + 10 = 0$.

Proof. Assume that the result is false; that is, assume that there is a real number x with $x^2 - 6x + 10 = 0$.

Then, by completing the square, we can write this as

$$(x-3)^2+1 = 0.$$

However $(x-3)^2 \geq 0$ for any real number x,

so the term $((x-3)^2)$ must be greater than or equal to 0.

So "$(x-3)^2$" + 1 must be greater than 0.

So $(x-3)^2+1 = 0$ is a contradiction.

Hence the original statement is true.

Example 2: Proof by Contradiction

- **Proposition.** Number $\sqrt{2}$ is irrational. Given that if a^2 is even, a must be even.

Proof. Suppose for the sake of contradiction that it is not true that $\sqrt{2}$ is irrational. Then $\sqrt{2}$ is rational, so there are integers *a, b* for which

$$\sqrt{2} = \frac{a}{b}.$$

Let this fraction be fully reduced, which means *a* and *b* are not both even, for if they were, the fraction could be further reduced by factoring 2's from the numerator and denominator and canceling. Squaring both sides of the eqt gives $2 = \frac{a^2}{b^2}$,

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

The above means a^2 is even (because $2b^2$). We assume *a, b* are not both even, so it implies b^2 is odd **and *b* is odd**.

Now since *a* is even there is an integer c for which *a*=2*c*. Plugging this value for "*a*" into $a^2 = 2b^2$, we get

$(2c)^2 = 2b^2$, or $4c^2 = 2b^2$, hence $b^2 = 2c^2$.

This means b^2 is even, so *b* is even (given fact in the question).

But previously **we deduced *b* is odd**.

Thus we have a contradiction b is even and b is odd.

Thus, our assumption that $\sqrt{2}$ is rational is false.

The number $\sqrt{2}$ is irrational .

Example 3: Proof by Contradiction

- **Proposition.** There are infinitely many prime numbers. Given that any natural number a has at least one prime divisor.

Proof. For the sake of contradiction, suppose there are only finitely many prime numbers. Then we can list all the prime numbers as p_1, p_2, p_3, p_4, p_n, where p_1=2, $p_2 = 3, p_3 = 5, p_4 = 7$ and so on and p_n is the largest prime number.

Now consider a= $(p_1 p_2 p_3 p_4 \dots p_n)$ +1, that is a is the product of all prime numbers plus 1.

Now a has at least one prime divisor (the above given fact), $p_{k,}$ $(p_{k,}|a)$.

Thus a= cp_k which means a= $(p_1 p_2 p_3 p_4 \dots p_n)$ +1= cp_k.

Divide both side by p_k gives us

$$(p_1 p_2 p_3 p_4 \dots p_{k-1} p_{k+1 \dots} p_n) + \frac{1}{p_k} = c$$

So $\frac{1}{p_k}$ = c -$(p_1 p_2 p_3 p_4 \dots p_{k-1} p_{k+1 \dots} p_n)$

The expression on the right is an integer, while the expression on the left is not an integer. This CANNOT be equal, CONTRADICTION.

So our assumption that there are only finitely many prime numbers is FALSE.

So there are infinitely many prime numbers.

Mathematical Induction

- Mathematical Induction can be used to prove statements that assert that *P(n)* is true for all positive integers *n*, where *P(n)* is a propositional function.
- It has two parts
  - A basic step, where we show *P(1)* is true.
  - An inductive step, where we show that for all +ve integers *k*, if *P(k)* is true, we show *p(k+1)* is true.

Example 1: Mathematical Induction

Prove by mathematical induction that for all positive integers n

$$1 + 2 + 3 + \cdots + n = n(n+1)/2$$

Solution. 1) For $n = 1$, we have $1 = 1 \cdot \frac{1+1}{2} = 1$， therefore $P(1)$ holds,

2) Assume that the statement is true for a particular value $n = k$, that is

$$1 + 2 + 3 + \cdots + k = k(k+1)/2$$

3) Prove that the sum is true for $n = k + 1$, that is

$$1 + 2 + 3 + \cdots + (k+1) = (k+1)(k+2)/2$$

If, to the left and right side of the equality 2) we add $k + 1$ increased is given series by next term

$$1 + 2 + 3 + \cdots + k + (k+1) = \frac{k(k+1) + 2(k+1)}{2} = (k+1)(k+2)/2$$

Therefore， the given statement is true for all positive integers.

Example 2: Mathematical Induction

Prove by mathematical induction that for all positive integers n

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

Solution. 1) For $n = 1$, we have $2 \cdot 1 - 1 = 1$^2， therefore $P(1)$ holds,

2) Assume that the statement is true for a particular value $n = k$, that is

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2$$

3) Prove that the sum is true for $n = k + 1$, that is

$$1 + 3 + 5 + \cdots + (2(k + 1) - 1) = (k + 1)^2$$

If, to the left and right side of the equality 2) we add $2k + 1$ increased is given series by next term

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + 2k + 1 = (k + 1)^2$$

Thus, the given statement is true for all positive integers.

Example 3: Mathematical Induction

Prove by mathematical induction that for all positive integers n

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = n(n+1)(2n+1)/6$$

Solution. 1) For $n = 1$, we have $1^2 = 1 \cdot \frac{(1+1)(2\cdot 1+1)}{6} = 6/6 = 1$, therefore $P(1)$ holds,

2) Assume that the statement is true for a particular value $n = k$, that is

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = k(k+1)(2k+1)/6$$

3) Prove that the sum is true for $n = k + 1$, that is

$$1^2 + 2^2 + 3^2 + \cdots + (k+1)^2 = (k+1)(k+2)(2k+3)/6$$

If, to the left and right side of the equality 2) we add$(k+1)^2$ increased is given series by next term

$$1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= \frac{(k+1)(2k^2 + 7k + 6)}{6} = (k+1)(k+2)(2k+3)/6$$

Therefore， the given statement is true for all positive integers.

Example 4: Mathematical Induction

Summing a Geometric Progression

Let r be a fixed real number. Then

$1 + r + r^2 + r^3 + \ldots + r^n = \dfrac{1 - r^{n+1}}{1 - r}$. This is $P(n)$.

Proof

Clearly $P(0)$ is true. (Note that we can anchor the induction where we like.)

So we suppose that $P(k)$ is true and we'll try and prove $P(k + 1)$.

So look at $\left(1 + r + r^2 + r^3 + \ldots + r^k\right) + r^{k+1}$.

By $P(k)$ the term in brackets is $\dfrac{1 - r^{k+1}}{1 - r}$ and so we can simplify this to

$$\frac{1 - r^{k+1}}{1 - r} + r^{k+1} = \frac{1 - r^{k+1} + r^{k+1} - r^{k+2}}{1 - r} = \frac{1 - r^{k+2}}{1 - r}$$ which is what

$P(k + 1)$ predicts. $\square$

END