

1.5 Rules of Inference

1.6 Introduction to Proofs

Dr Patrick Chan

School of Computer Science and Engineering
South China University of Technology

Recall...

- John is a cop. John knows first aid. Therefore, all cops know first aid



Agenda

- Rules of Inference
- Rules of Inference for Quantifiers

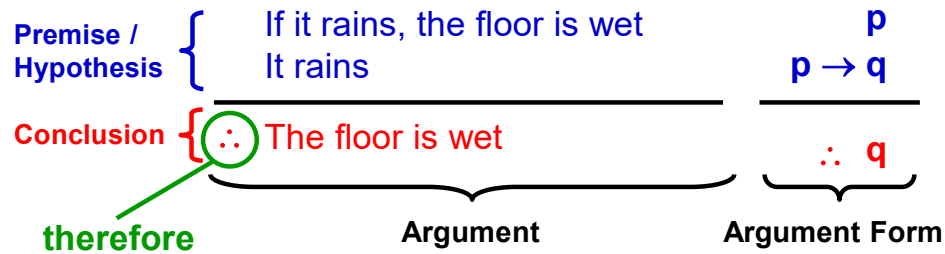
Recall...

- Some students work hard to study. Some students fail in examination. So, some work hard students fail in examination.



Argument

p: It rains
q: The floor is wet

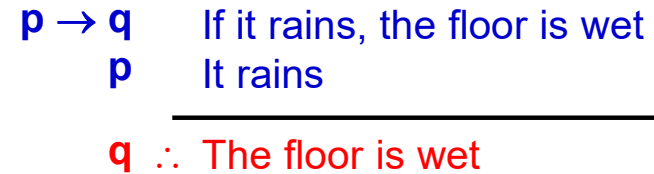


- Argument in propositional logic is a sequence of propositions
 - Premises / Hypothesis: All except the final proposition
 - Conclusion: The final proposition
- Argument form represents the argument by variables

Argument

- Example:

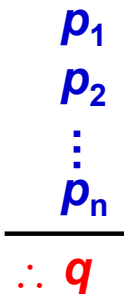
Argument is valid



$(p \wedge (p \rightarrow q)) \rightarrow q$				Tautology	
Need to check if the conclusion is true or not	p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$(p \wedge (p \rightarrow q)) \rightarrow q$
Must be true	T	T	T	T	T
	T	F	F	F	T
	F	T	T	F	T
	F	F	T	F	T

Argument: Valid?

- Given an argument, where
 - p_1, p_2, \dots, p_n be the premises
 - q be the conclusion
- The argument is valid when $(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow q$ is a tautology
 - When all premises are true, the conclusion should be true
 - When not all premises are true, the conclusion can be either true or false



p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Focus on this case
Check if it happens

Rules of Inference

- How to show an argument is valid?
 - Truth Table
 - May be tedious when the number of variables is large
 - Rules of Inference
 - Firstly establish the validity of some relatively simple argument forms, called rules of inference
 - These rules of inference can be used as building blocks to construct more complicated valid argument forms

Rules of Inference

Modus Ponens

- Affirm by affirming

$$\frac{p \quad p \rightarrow q}{\therefore q}$$

Modus Tollens

- Deny by denying

$$\frac{\neg q \quad p \rightarrow q}{\therefore \neg p}$$

Rules of Inference

Addition

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

Simplification

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

Conjunction

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

Rules of Inference

Hypothetical Syllogism

$$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$$

Disjunctive Syllogism

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

Rules of Inference

Resolution

$p = T$	$p = F$
$q = T/F$	$q = T$
$r = T$	$r = T/F$

$$\frac{p \vee q \quad \neg p \vee r}{\therefore q \vee r}$$

Example

- I go to swim or I play tennis
- I do not go to swim or I play football
- Therefore, I play tennis or I play football

Rules of Inference (\rightarrow)

Modus Ponens	$((p \rightarrow q) \wedge (p)) \rightarrow q$
Modus Tollens	$((\neg q) \wedge (p \rightarrow q)) \rightarrow \neg p$
Hypothetical Syllogism	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$
Disjunctive Syllogism	$((p \vee q) \wedge (\neg p)) \rightarrow q$
Addition	$(p) \rightarrow p \vee q$
Simplification	$((p) \wedge (q)) \rightarrow p$
Conjunction	$((p) \wedge (q)) \rightarrow (p \wedge q)$
Resolution	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$

Comparison between Inference and Equivalence

- Inference ($p \rightarrow q$)**
 - Meaning:** If p, then q
 - $p \rightarrow q$ does **not** mean $q \rightarrow p$
 - Either **inference** or **equivalence** rules can be used
 - $p \leftrightarrow q$ implies $p \rightarrow q$
 - \Rightarrow is used in proof
- Equivalence ($p \leftrightarrow q$)**
 - Meaning:** p is equal to q
 - $p \leftrightarrow q$ mean $q \leftrightarrow p$
 - Only equivalence** rules can be used
 - $p \leftrightarrow q$ can be proved by showing $p \rightarrow q$ and $q \rightarrow p$
 - \Leftrightarrow is used in proof
- Equivalence (\leftrightarrow) is a **more restrictive** relation than Inference (\rightarrow)

Rules of Equivalence (\leftrightarrow)

- Recall...

Identify Laws	$p \wedge T \equiv p$ $p \vee F \equiv p$
Domination Laws	$p \vee T \equiv T$ $p \wedge F \equiv F$
Idempotent Laws	$p \vee p \equiv p$ $p \wedge p \equiv p$
Negation Laws	$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$
Double Negation Law	$\neg(\neg p) \equiv p$
Commutative Laws	$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$
Associative Laws	$p \vee (q \vee r) \equiv (p \vee q) \vee r$ $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
Distributive Laws	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Absorption Laws	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$
De Morgan's Laws	$\neg(p \vee q) \equiv \neg p \wedge \neg q$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$

Using Rules of Inference

- Example 1:
 - Given:**
 - 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
 - Can these propositions lead to the **conclusion** "We will be home by sunset" ?

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

- $\neg p \wedge q$ ■ It is **not** sunny this afternoon **and** it is colder than yesterday
 - $r \rightarrow p$ ■ We will go swimming **only if** it is sunny
 - $\neg r \rightarrow s$ ■ **If** we do **not** go swimming, **then** we will take a canoe trip
 - $s \rightarrow t$ ■ **If** we take a canoe trip, **then** we will be home by sunset
-
- t ■ We will be home by sunset

Using Rules of Inference

- Or, another presentation method:

Hypothesis:

$$\neg p \wedge q \quad \Rightarrow (\neg p \wedge q) \wedge (r \rightarrow p) \wedge (\neg r \rightarrow s) \wedge (s \rightarrow t)$$

$$r \rightarrow p \quad \Rightarrow \neg p \wedge (r \rightarrow p) \wedge (\neg r \rightarrow s) \wedge (s \rightarrow t) \quad \text{By Simplification}$$

$$\neg r \rightarrow s \quad \Rightarrow \neg r \wedge (\neg r \rightarrow s) \wedge (s \rightarrow t) \quad \text{By Modus Tollens}$$

$$s \rightarrow t \quad \Rightarrow s \wedge (s \rightarrow t) \quad \text{By Modus Ponens}$$

Conclusion:

$$t \quad \Rightarrow t \quad \text{By Modus Ponens}$$

Using Rules of Inference

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

Therefore, the propositions can lead to the conclusion
 We will be home by sunset

😊 Small Exercise 😊

- **Given:**
 - 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
 - If I go to sleep early, then I will wake up feeling refreshed
- Can these propositions lead to the **conclusion** "If I do not finish writing the program, then I will wake up feeling refreshed."

Let p: you send me an e-mail message
 q: I will finish writing the program
 r: I will go to sleep early
 s: I will wake up feeling refreshed

- $p \rightarrow q$ ■ If you send me an e-mail message, then I will finish writing the program
 - $\neg p \rightarrow r$ ■ If you do not send me an e-mail message, then I will go to sleep early
 - $r \rightarrow s$ ■ If I go to sleep early, then I will wake up feeling refreshed
-
- $\neg q \rightarrow s$ ■ If I do not finish writing the program, then I will wake up feeling refreshed

😊 Small Exercise 😊

- Or, another presentation method:

Hypothesis:

$$p \rightarrow q \quad (p \rightarrow q) \wedge (\neg p \rightarrow r) \wedge (r \rightarrow s)$$

$$\neg p \rightarrow r \quad \Leftrightarrow (\neg q \rightarrow \neg p) \wedge (\neg p \rightarrow r) \wedge (r \rightarrow s) \quad \text{Contrapositive}$$

$$r \rightarrow s$$

$$\Rightarrow (\neg q \rightarrow r) \wedge (r \rightarrow s) \quad \text{By Hypothetical Syllogism}$$

Conclusion:

$$\neg q \rightarrow s \quad \Rightarrow (\neg q \rightarrow s) \quad \text{By Hypothetical Syllogism}$$

😊 Small Exercise 😊

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)

Hypothesis:

$$p \rightarrow q$$

$$\neg p \rightarrow r$$

$$r \rightarrow s$$

Conclusion:

$$\neg q \rightarrow s$$

Therefore, the propositions can lead to the conclusion
 If I do not finish writing the program,
 then I will wake up feeling refreshed

Using Rules of Inference Fallacies

- Are the following arguments correct?

- **Example 1 (Fallacy of affirming the conclusion)**

Hypothesis

- If you success, you work hard

$$p \rightarrow q$$

- You work hard

$$q$$

Conclusion

- You success

$$\therefore p$$



- **Example 2 (Fallacy of denying the hypothesis)**

Hypothesis

- If you success, you work hard

$$p \rightarrow q$$

- You do not success

$$\neg p$$

Conclusion

- You do not work hard

$$\therefore \neg q$$



Rules of Inference for Quantifiers

Universal Instantiation

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

where a is a particular member of the domain

Existential Instantiation

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

Universal Generalization

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

Existential Generalization

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

Be noted that b that we select must be an arbitrary, and not a specific

Let	DC(x):	x studies in discrete mathematics
	CS(x):	x studies in computer science
	Domain of x:	student

$$\forall x (DC(x) \rightarrow CS(x))$$

$$DC(\text{Marla})$$

$$CS(\text{Marla})$$

- Everyone in this discrete mathematics class has taken a course in computer science
- Marla is a student in this class
- Marla has taken a course in computer science

Rules of Inference for Quantifiers

Example 1

Given

- Everyone in this discrete mathematics class has taken a course in computer science
- Marla is a student in this class

- These premises imply the **conclusion**
"Marla has taken a course in computer science"

Rules of Inference for Quantifiers

Premise:

$$\forall x (DC(x) \rightarrow CS(x))$$

$$DC(\text{Marla})$$

Conclusion:

$$CS(\text{Marla})$$

Step	Reason
1. $\forall x (DC(x) \rightarrow CS(x))$	Premise
2. $DC(\text{Marla}) \rightarrow CS(\text{Marla})$	Universal Instantiation from (1)
3. $DC(\text{Marla})$	Premise
4. $CS(\text{Marla})$	Modus ponens using (2) and (3)

Therefore, the propositions can lead to the conclusion
Marla has taken a course in computer science

Using Rules of Inference for Quantifiers

- Or, another presentation method:

Premise:

$$\forall x (DC(x) \rightarrow CS(x))$$

$$DC(Marla)$$

Conclusion:

$$CS(Marla)$$

$$\forall x (DC(x) \rightarrow CS(x)) \wedge DC(Marla)$$

By Universal Instantiation

$$\Rightarrow (DC(Marla) \rightarrow CS(Marla)) \wedge DC(Marla)$$

$$\Rightarrow CS(Marla) \quad \text{By Modus ponens}$$

Let	C(x):	x in this class
	RB(x):	x reads the book
	PE(x):	x passes the first exam
	Domain of x:	any person

$$\exists x (C(x) \wedge \neg RB(x))$$

- A student in this class has **not** read the book

$$\forall x (C(x) \rightarrow PE(x))$$

- Everyone** in this class passed the first exam

$$\exists x (PE(x) \wedge \neg RB(x))$$

- Someone** who passed the first exam has **not** read the book

We cannot define the domain as student in this class since the conclusion means anyone

😊 Small Exercise 😊

Given

- A student in this class has not read the book
- Everyone in this class passed the first exam

- These premises imply the **conclusion**

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

😊 Small Exercise 😊

Premise:

$$\exists x (C(x) \wedge \neg RB(x))$$

$$\forall x (C(x) \rightarrow PE(x))$$

Conclusion:

$$\exists x (PE(x) \wedge \neg RB(x))$$

Step	Reason
$\exists x (C(x) \wedge \neg RB(x))$	Premise
$C(a) \wedge \neg RB(a)$	Existential Instantiation from (1)
$C(a)$	Simplification from (2)
$\forall x (C(x) \rightarrow PE(x))$	Premise
$C(a) \rightarrow PE(a)$	Universal Instantiation from (4)
$PE(a)$	Modus ponens from (3) and (5)
$\neg RB(a)$	Simplification from (2)
$PE(a) \wedge \neg RB(a)$	Conjunction from (6) and (7)
$\exists x (PE(x) \wedge \neg RB(x))$	Existential Generalization from (8)

Therefore, the propositions can lead to the conclusion
Someone who passed the first exam has not read the book

☺ Small Exercise ☺

- Or, another presentation method:

$$(\exists x (C(x) \wedge \neg RB(x))) \wedge (\forall x (C(x) \rightarrow PE(x)))$$

$$\Rightarrow C(a) \wedge \neg RB(a) \wedge (\forall x (C(x) \rightarrow PE(x))) \quad \text{By Existential Instantiation}$$

$$\Rightarrow C(a) \wedge \neg RB(a) \wedge (C(a) \rightarrow PE(a)) \quad \text{By Universal Instantiation}$$

$$\Rightarrow PE(a) \wedge \neg RB(a) \quad \text{By Modus ponens}$$

$$\Rightarrow \exists x (PE(x) \wedge \neg RB(x)) \quad \text{By Existential Generalization}$$

Premise:
 $\exists x (C(x) \wedge \neg RB(x))$
 $\forall x (C(x) \rightarrow PE(x))$

Conclusion:
 $\exists x (PE(x) \wedge \neg RB(x))$

Combining Rules of Inference

- Example:

- Given**

- For all positive integers n,
if n is greater than 4, then n² is less than 2ⁿ
is **true**.

- Show** that $100^2 < 2^{100}$

Combining Rules of Inference

- The rules of inference of Propositions and Quantified Statements can be combined

- Universal Modus Ponens**

$$\forall x (P(x) \rightarrow Q(x))$$

$P(a)$, where a is a particular
element in the domain

$$\therefore Q(a)$$

$$(\forall x (P(x) \rightarrow Q(x))) \wedge (P(a))$$

By **Universal Instantiation**

$$\Rightarrow (P(a) \rightarrow Q(a)) \wedge (P(a))$$

By **Modus Ponens**

$$\Rightarrow Q(a)$$

- Universal Modus Tollens**

$$\forall x (P(x) \rightarrow Q(x))$$

$\neg Q(a)$, where a is a particular
element in the domain

$$\therefore \neg P(a)$$

$$(\forall x (P(x) \rightarrow Q(x))) \wedge (\neg Q(a))$$

By **Universal Instantiation**

$$\Rightarrow (P(a) \rightarrow Q(a)) \wedge (\neg Q(a))$$

By **Modus Tollens**

$$\Rightarrow \neg P(a)$$

Combining Rules of Inference

- Example:

For **all** positive integers n,
if n is greater than 4, **then** n² is less than 2ⁿ

$$P(n): n > 4$$

$$Q(n): n^2 < 2^n$$

$$\forall n (P(n) \rightarrow Q(n))$$

$$P(100) \quad (\text{since } 100 > 4)$$

$$\therefore Q(100) \quad (100^2 < 2^{100}) \quad \text{By Universal Modus Ponens}$$

Summary

- What we have learnt in previous lectures?
 - Proposition
 - Operator
 - Predicates
 - Quantifier
 - Truth Table
 - Rules of Equivalence
 - Rules of Inference
- } Show if an argument is valid
- This is called the **formal proof**
 - very clear and precise
 - extremely long and hard to follow

Informal Proofs

- In **practice**, the **proofs of theorems** designed for human consumption are almost **always informal proofs**
 - More than one rule** of inference may be used in each step
 - Steps** may be **skipped**
 - The **axioms** being **assumed**
 - e.g. even number can be written as $2k$, where k is integer
 - The **rules** of inference used are **not explicitly stated**

Informal Proofs

- Informal proofs** can often **explain to humans** why **theorems are true**
 - Proof of mathematical theorems
 - Applications to computer science
- Move from **formal proofs** toward more **informal proofs**



Proof for Theorems

- Types of Theorem**
 - Implication ($P(x) \rightarrow Q(x)$)
 - Equivalence ($P(x) \leftrightarrow Q(x)$)
 - Statement ($P(x)$)
- Type of proof**
 - Universal Quantification (For all...)
 - Existential Quantification (For some...)
 - Uniqueness Quantification (Only one...)

Proof for Theorems: Methods

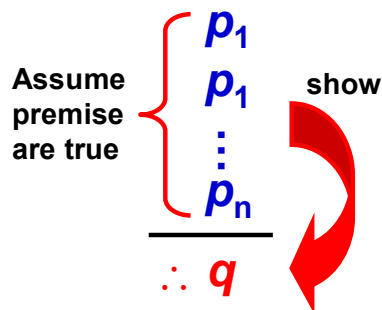
- **Implication** ($P(x) \rightarrow Q(x)$)
 - **Direct Proof**
Assume $P(x)$ is true, show $Q(x)$ is true
 - **Indirect Proof: Proof by Contraposition**
Assume $\neg Q(x)$ is true and show $\neg P(x)$ is true
- **Equivalence** ($P(x) \leftrightarrow Q(x)$)
 - As $P(x) \leftrightarrow Q(x) \equiv (P(x) \rightarrow Q(x)) \wedge (Q(x) \rightarrow P(x))$
- **Statement** ($P(x)$)
 - **Indirect Proof: Proof by Contradiction**

Direct Proof: Example 1

- Prove “If n is an odd integer, then n^2 is odd”
- Given,
 - The integer n is **even**
if there exists an **integer** k such that $n = 2k$
 - The integer n is **odd**
if there exists an **integer** k such that $n = 2k+1$

Direct Proof

- **Direct proofs** lead **from the hypothesis** of a theorem **to the conclusion**
 1. Assume the premises are true
 2. Show the conclusion is true



Show
If n is an odd integer, then n^2 is odd

1. Assume the hypothesis is true
“ n is odd” is true
 - By definition, $n = 2k + 1$, where k is a integer
2. Show the conclusion is correct
 n^2 is odd

$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

 - By definition, as $(2k^2 + 2k)$ is an **integer** we can conclude that n^2 is an **odd integer**
- Therefore, “if n is an odd integer, then n^2 is an odd integer” has been proved

Direct Proof: Example 2

- Prove “If m and n are both perfect squares, then nm is also a perfect square”
- Given
 - An integer a is a perfect square if there is an integer b such that $a = b^2$

Direct Proof: Example 3

- Prove “if n is an integer and $3n + 2$ is odd, then n is odd”
- Assume $3n + 2$ is an odd integer
 - $3n + 2 = 2k + 1$ for some integer k
- Show that n is odd

$$3n + 2 = 2k + 1$$

$$3n = 2k - 1$$

$$n = \frac{2k - 1}{3}$$



Show
If m and n are both perfect squares, then nm is also a perfect square

1. Assume m and n are both perfect squares
 - By definition, $m = a^2$ and $n = b^2$, where a and b are integers
 2. Show that mn is a perfect square
 - $mn = a^2b^2 = (ab)^2$, where ab is an integer
 - By the definition, we can conclude that mn is a perfect square
- Therefore, “An integer a is a perfect square if there is an integer b such that $a = b^2$ ” has been proved

Indirect Proof

- Sometimes, direct proofs may reach dead ends
- Indirect proof may help
 - Prove theorems not directly
 - Do not start with the hypothesis and end with the conclusion

Proof by Contraposition

- Recall, contrapositive:

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

- $p \rightarrow q$ can be proved by showing $\neg q \rightarrow \neg p$ is true

- Assume the conclusion is not true
- Show either one premise is not true

$$(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow q$$

$$\equiv \neg q \rightarrow \neg(p_1 \wedge p_2 \wedge \dots \wedge p_n)$$

$$\equiv \neg q \rightarrow (\neg p_1 \vee \neg p_2 \vee \dots \vee \neg p_n)$$

Proof by Contraposition: Example 2

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

1. Assume $a > \sqrt{n}$ and $b > \sqrt{n}$ is true

2. Show $n \neq ab$

- $ab > (\sqrt{n})^2 = n$
- Therefore, $ab \neq n$

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

Proof by Contraposition: Example 1

- Prove “if n is an integer and $3n + 2$ is odd, then n is odd”

1. Assume the conclusion is false

n is not odd

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

- $n = 2k$, where k is an integer

2. Show that the premises are not correct

$3n + 2$ is not odd

- $3(2k) + 2 = 6k + 2 = 2(3k + 1)$

- As if n is not odd, $3n + 2$ is not odd
Therefore, if n is an integer and $3n + 2$ is odd, then n is odd

😊 Small Exercise 😊

- Prove that “the sum of two rational numbers is rational”

Given

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

😊 Small Exercise 😊

■ Direct Proof

- Suppose that r and s are rational numbers

- $r = p/q$, $s = t/u$, where $q \neq 0$ and $u \neq 0$

- Show that $r+s$ is rational number

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu}$$

- As $q \neq 0$ and $u \neq 0$, $qu \neq 0$
 - Therefore, $r + s$ is rational
- Therefore, direct proof succeeded

😊 Small Exercise 😊

■ Proof by contraposition

- Suppose n is not odd

- $n = 2k$, where k is an integer

- Show n^2 is not even

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

- n^2 is even

- Therefore, proof by contraposition succeeded

😊 Small Exercise 😊

- Prove “if n is an integer and n^2 is odd, then n is odd”

■ Direct proof

- Suppose that n is an integer and n^2 is odd

- Exists an integer k such that $n^2 = 2k + 1$

- Show n is odd

- Show $(n = \pm \sqrt{2k + 1})$ is odd

- May not be useful

Universal Quantification

Proof of Theorems: Equivalence

- Recall, $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

- To prove equivalence, we can show $p \rightarrow q$ and $q \rightarrow p$ are both true

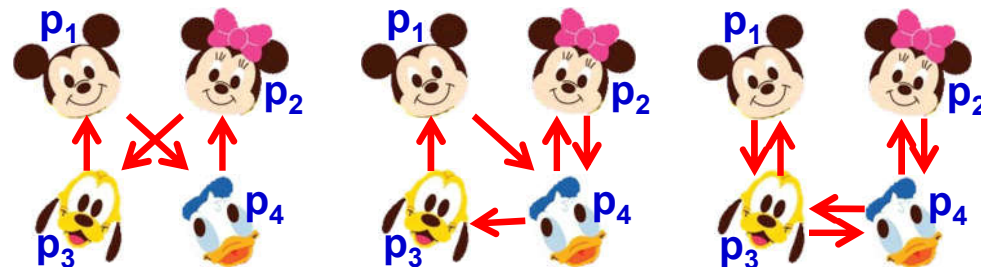
Equivalence: Example

- Prove “If n is a positive integer, then n is odd if and only if n^2 is odd”
- Two steps
 - If n is a positive integer, if n is odd, then n^2 is odd (shown in slides 43)
 - If n is a positive integer, if n^2 is odd, then n is odd (shown in slides 54)
- Therefore, it is true

Proof of Theorems: Equivalence

$$p_1 \leftrightarrow p_2 \leftrightarrow p_3 \leftrightarrow \dots \leftrightarrow p_n$$

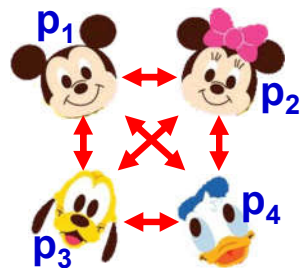
- When proving a group of statements are equivalent, any chain of conditional statements can be established as long as it is possible to work through the chain to go from anyone of these statements to any other statement



Proof of Theorems: Equivalence

- How to show p_1, p_2, p_3 and p_4 are equivalence?

- $p_1 \leftrightarrow p_2$
- $p_1 \leftrightarrow p_3$
- $p_1 \leftrightarrow p_4$
- $p_2 \leftrightarrow p_3$
- $p_2 \leftrightarrow p_4$
- $p_3 \leftrightarrow p_4$



- Not necessary

- E.g. if $p_1 \leftrightarrow p_2$ and $p_2 \leftrightarrow p_3$, then $p_1 \leftrightarrow p_3$

Statement: Example



Can you prove “You love me” ? p

How?

If you love me, $p \rightarrow q$ you will buy me iphone5



What does it mean if you...

- Buy iphone q Prove nothing
- Do not buy iphone

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



Universal Quantification: Methods of Proving Theorems Statement: Example (Correct)

Can you prove "You love me" ? p

How?

If you do not love me,
you will not buy me iphone5

$\neg p \rightarrow \neg q$

What does it mean if you...

1. Buy iphone $q \rightarrow p$

2. Do not buy iphone

$\neg q$ Prove nothing



Universal Quantification: Methods of Proving Theorems: Statement Proof by Contradiction

- Procedures of Proof by Contradiction to prove p is correct :
 - Understand the meaning of $\neg p$
 - Find out what $\neg p$ implies ($\neg p \rightarrow q$ is true)
 - Show that q is not correct

Universal Quantification: Methods of Proving Theorems: Statement Proof by Contradiction

- By using **Proof by Contradiction**,
If you want to show p is true, you need:

- $\neg p \rightarrow q$ is true
- q is false

$\neg P$	Q	$\neg P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

- Recall, **Proof by Contradiction** of $p \rightarrow q$ is
 $\neg p \rightarrow q$

Universal Quantification: Methods of Proving Theorems: Statement Proof by Contradiction: Example 1

- Prove $\sqrt{2}$ is irrational

Not "if... then..." format
Only one statement

- Understand the meaning of $\neg p$

$\sqrt{2}$ is rational

- Find out what $\neg p$ implies

If $\sqrt{2}$ is rational, there exist integers p and q with
 $\sqrt{2} = p / q$, where p and q have no common factors

- So that the fraction p / q is in lowest terms

- Show that q is not correct

Show "there exist integers p and q with $\sqrt{2} = p / q$ "
is not true

Show "there exist integers p and q with $\sqrt{2} = p / q$ " is not true

$$\sqrt{2} = p / q \quad , \text{ where } q \neq 0$$

$$2q^2 = p^2$$

- p^2 is an even number
- If p^2 is even, so $p = 2a$, and a is an integer

$$2q^2 = 4a^2$$

$$q^2 = 2a^2$$
- q is also even
- As p and q are even, they have a common factor 2, which leads the contradiction
- Therefore, " $\sqrt{2}$ is irrational" is true

Let p : "At least four of 22 chosen days fall on the same day of the week."

1. Understand the meaning of $\neg p$

At most three of 22 chosen days fall on the same day of the week

2. Find out what $\neg p$ implies

As at most three day fall on the same week day, therefore a week should have at least $22 / 3$ days

3. Show that q is not correct

A week only has 7 days, therefore, q is not correct

Therefore, p is correct

Universal Quantification: Methods of Proving Theorems: Statement
Proof by Contradiction: Example 2

- Show that at least four of any 22 days must fall on the same day of the week.

July

W	S	M	T	W	T	F	S
19						1	2
20	3	4	5	6	7	8	9
21	10	11	12	13	14	15	16
22	17	18	19	20	21	22	23
23	24	25	26	27	28	29	30
24	31						

Universal Quantification: Methods of Proving Theorems: Statement
Proof by Contradiction

- Proof by Contradiction can also be used to show $P(x) \rightarrow Q(x)$ (implication)
- Let $S(x) : P(x) \rightarrow Q(x)$ and prove $S(x)$ is correct
 - $S(x) : P(x) \rightarrow Q(x)$
 - $\neg S(x) \rightarrow (P(x) \wedge \neg Q(x))$ is true
 - $P(x) \wedge \neg Q(x)$ is false

$$\begin{aligned} &\neg S(x) \\ &= \neg(P(x) \rightarrow Q(x)) \\ &= \neg(\neg P(x) \vee Q(x)) \\ &= P(x) \wedge \neg Q(x) \end{aligned}$$

Proof by Contradiction: Example 3

- Show "If $3n + 2$ is odd, then n is odd"
 - Be noted that proof by contraposition can be used (shown in slide 50)*
- Let $P(n): Q(3n+2) \rightarrow Q(n)$, where $Q(n) : "n \text{ is odd}"$
- $\neg P(n)$ implies:
 - $\neg P(n) \equiv \neg(Q(3n+2) \rightarrow Q(n))$
 - $\equiv \neg(\neg Q(3n+2) \vee Q(n))$
 - $\equiv Q(3n+2) \wedge \neg Q(n)$

Exhaustive Proof and Proof by Cases

- Sometimes, a theorem **cannot be proved easily using** a single argument that holds for **all possible cases**
- Rather than considering $(p \rightarrow q)$ directly, we can **consider different cases separately**
- This argument is named **Proof by Cases**:
 - $$(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$$
 - $$\equiv [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)]$$
- E.g. $x^2 \geq 0$, we can $x < 0$, $x = 0$ and $x > 0$

Proof by Contradiction: Example 3

- $\neg P(n)$ implies " $Q(3n+2) \wedge \neg Q(n)$ "
 - $\neg Q(n)$ imply...
 - n is even, $n = 2k$, where k is integer
 - $3n+2 = 3(2k)+2 = 2(3k+1)$
 - Therefore, $3n+2$ is even ($\neg Q(3n+2)$)
 - $Q(3n+2) \wedge \neg Q(3n+2)$ is false
 - Therefore, $\neg P(n)$ must be false
 - Therefore,
 - $Q(3n+2) \rightarrow Q(n)$ is true

Exhaustive Proof

- **Exhaustive Proofs**
 - **Prove all the possibilities**
 - Example
 - Prove that $(n + 1)^3 > 3^n$ if n is a positive integer with $n \leq 4$
 - Prove all the possibilities: $n = 1, 2, 3$ and 4

Exhaustive Proof: Example 1

- Prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$

When $n = 1$

LHS: $(n + 1)^3 = 8$

RHS: $3^n = 3$

LHS > RHS

When $n = 2$

LHS: $(n + 1)^3 = 27$

RHS: $3^n = 9$

LHS > RHS

When $n = 3$

LHS: $(n + 1)^3 = 64$

RHS: $3^n = 27$

LHS > RHS

When $n = 4$

LHS: $(n + 1)^3 = 125$

RHS: $3^n = 81$

LHS > RHS

- Therefore, $(n + 1)^3 > 3^n$ is valid

Proof by Cases

- Drawback of Exhaustive Proofs** is to check only a relatively small number of instances of a statement
- Proof by Cases**
 - Prove all situations
 - Example
 - Prove that if n is an integer, then $n^2 > n$
 - Prove all the situations: n is positive, equal and negative

Exhaustive Proof: Example 2

- Given
 - An integer is a **perfect power** if it equals n^a , where a is an integer greater than 1
- Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9
 - By exhaustive proof, list all the perfect powers not exceeding 100

	n=1	2	3	4	5	6	7	8	9	10
a=2	1	4	9	16	25	36	49	64	81	100
3	1	8	27	64						
4	1	32	81							
5	1	64								
>5	1									

- Therefore, only 8 and 9 are consecutive

Proof by Cases: Example 1

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

When $n \geq 1$

$n^2 = n \times n \geq n \times 1 = n$, therefore $n^2 \geq n$

When $n = 0$

$n^2 = n = 0$, therefore, $n^2 = n$

When $n \leq -1$

$n^2 > 0$ and $n < 0$, therefore $n^2 \geq n$

- Therefore, this theorem is valid

Proof by Cases: Example 2

- Use a proof by cases to show that $|x y| = |x| |y|$, where x and y are real numbers
(Recall $|a| = a$, when $a \geq 0$; $|a| = -a$ when $a < 0$)

When $x \geq 0$ and $y \geq 0$

$$|x y| = x y = |x| |y|$$

When $x < 0$ and $y \geq 0$

$$|x y| = -x y = (-x) (y) = |x| |y|$$

When $x \geq 0$ and $y < 0$

$$|x y| = -x y = (x) (-y) = |x| |y|$$

When $x < 0$ and $y < 0$

$$|x y| = x y = (-x) (-y) = |x| |y|$$

- Therefore, this theorem is valid

Existence Proofs

- Example:
 - Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways
 - After considerable computation (such as a computer search), we find that

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$
 - An example is given, the proof is done

Existence Proofs

- We will focus on the theorems which are assertions that objects of a particular type exist (\exists)
 - A theorem of this type is a proposition of the form $\exists x P(x)$, where P is a predicate
 - The proof of this proposition is **Existence Proof**
 - By finding an element a such that $P(a)$ is true

Uniqueness Proof

- The theorems which assert the existence of a unique element with a particular property will be discussed
- The two parts of a uniqueness proof are:
 - Existence** (An element with the property exists)
 - Show that an element x with the property exists
 - Uniqueness** (No other element has this property)
 - Show that if $y \neq x$, y does not have the property.
- Equivalently, we can show that if x and y both have the desired property, then $x = y$

$$\underbrace{\exists x (P(x))}_{\text{Existence}} \wedge \underbrace{\forall y (P(y) \rightarrow (y = x))}_{\text{Uniqueness}}$$

Uniqueness Proof: Example

- Show that if a and b are real numbers and $a \neq 0$, then there is a **unique real number** r such that $ar + b = 0$
- **Existence Part**
 - The real number $t = -b/a$ is a **solution** of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$
 - Consequently, a real number t exists for which $at + b = 0$
- **Uniqueness Part**
 - Suppose that s is a real number such that $as + b = 0$
$$at + b = as + b \quad t \text{ is } -b/a$$
$$at = as \quad a \text{ is nonzero}$$
$$t = s$$
 - This means that if $s \neq t$, then $as + b \neq 0$

Tips

- **DO NOT over simplify the proof**
 - “Obviously” or “clearly” in proofs indicate that steps have been **omitted** that the author **expects the reader to be able to fill in**
 - Unfortunately, this assumption is often **not warranted**
 - We will assiduously try to **avoid using these words** and try **not to omit too many steps**
- However, if we **included all steps** in proofs, our **proofs** would often be **too long**

