

# Logic and Proof

---

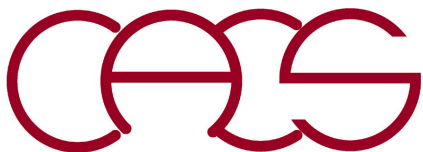
---

**Aiichiro Nakano**

*Collaboratory for Advanced Computing & Simulations  
Department of Computer Science  
Department of Physics & Astronomy  
Department of Quantitative & Computational Biology  
University of Southern California*

**Email: [anakano@usc.edu](mailto:anakano@usc.edu)**

From K. H. Rosen, *Discrete Mathematics and Its Applications*  
(McGraw-Hill) Chapter 1



# Logic

---

**Logic = mathematical foundation for:**

- Objective reasoning
- Formal proofs
- Computation

**Proposition:** A declarative sentence that is either true or false, but not both

(Example) ‘today is Friday’

‘read this book’ × — imperative

‘what time is it’ × — interrogative

**Predicate (propositional function):** A statement involving variables

(Example)  $P(x, y)$ : Student  $x$  has studied subject  $y$

**Truth value:** True (T) or false (F)

# Connectives (1)

Logical operators to form composite propositions from existing propositions

- **Negation**  
 $\neg p$ : “not  $p$ ”; inverts the truth value
- **Conjunction**  
 $p \wedge q$ : “ $p$  and  $q$ ”; T if both  $p$  and  $q$  are T
- **Disjunction**  
 $p \vee q$ : “ $p$  or  $q$ ”; F if both  $p$  and  $q$  are F, T otherwise
- **Exclusive or**  
 $p \oplus q$ : T when exactly one of  $p$  and  $q$  is T

**Truth table:** Combinatorial enumeration of the truth values of composite propositions;  $2^n$  rows for a  $n$ -proposition composite

Unary

$p$	$\neg p$
T	F
F	T

Binary

$p$	$q$	$p \wedge q$	$p \vee q$	$p \oplus q$
T	T	T	T	F
T	F	F	T	T
F	T	F	T	T
F	F	F	F	F

# Connectives (2)

**Implication:**  $p \rightarrow q$ ; F when  $p$  is T and  $q$  is F, and T otherwise  
                  hypothesis    conclusion

“if  $p$ , then  $q$ ” (“ $q$  if  $p$ ”)  
“ $p$  implies  $q$ ”  
“ $p$  is a sufficient condition for  $q$ ”

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

## Related implications

- **Contrapositive:**  $\neg q \rightarrow \neg p$
- **Converse:**  $q \rightarrow p$
- **Inverse:**  $\neg p \rightarrow \neg q$

**Biconditional:**  $p \leftrightarrow q$ ; T if  $p$  and  $q$  has the same truth value

“ $q$  if and only if (iff)  $p$ ”  
“ $p$  is sufficient and necessary for  $q$ ”

$p$	$q$	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

# Nested Connectives

- Use parenthesis

$$(p \wedge q) \vee r$$

- Precedence: No need to memorize, except for

$$\neg p \wedge q \text{ is } (\neg p) \wedge q \text{ not } \neg(p \wedge q)$$

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

operate first



operate last

# Logical Equivalences

- **Tautology:** A compound proposition that is always T
- $p \equiv q$ :  $p$  and  $q$  are logically equivalent;  $p \leftrightarrow q$  is a tautology  
Syntactically different composite propositions can have the same meaning (truth values)

Truth table can be used to determine the equivalence

(Example) “equivalence of contrapositive”

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

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

Equivalent

# Basic Logical Equivalences (1)

---

---

Useful to simplify complex composite propositions

$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	<b>Identity laws</b>
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	<b>Domination laws</b>
$p \vee p \equiv p$ $p \wedge p \equiv p$	<b>Idempotent laws</b>
$\neg(\neg p) \equiv p$	<b>Double negation</b>

# Basic Logical Equivalences (2)

$\wedge$  and  $\vee$  are commutative, associative, and distributive

$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$	<b>Commutative laws</b>
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	<b>Associative laws</b>
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	<b>Distributive laws</b>

**Associative laws make the following well defined**

- $p_1 \wedge p_2 \wedge \dots \wedge p_n$       **T if all are T**
- $p_1 \vee p_2 \vee \dots \vee p_n$       **T if one is T**



# Basic Logical Equivalences (3)

$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

## Generalized De Morgan's theorem

- $\neg(p_1 \wedge p_2 \wedge \dots \wedge p_n) \equiv \neg p_1 \vee \neg p_2 \vee \dots \vee \neg p_n$   
“it is not the case that all are T”  $\equiv$  “one is F”
- $\neg(p_1 \vee p_2 \vee \dots \vee p_n) \equiv \neg p_1 \wedge \neg p_2 \wedge \dots \wedge \neg p_n$   
“it is not the case that one is T”  $\equiv$  “all are F”

# Basic Logical Equivalences (4)

---

---

Equivalences involving implication & biconditional  
in terms of other connectives

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

$$p \rightarrow q \equiv \neg q \rightarrow \neg p \text{ (contrapositive)}$$

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

# Basic Logical Equivalences (5)

---

Additional logical equivalences can be derived, combining other logical equivalences that have already been established

**(Example)** Show that  $(p \wedge q) \rightarrow (p \vee q) \equiv T$   
*i.e.*, “ $(p \wedge q) \rightarrow (p \vee q)$  is a tautology”

$(p \wedge q) \rightarrow (p \vee q) \equiv \neg(p \wedge q) \vee (p \vee q)$	$p \rightarrow q \equiv \neg p \vee q$
$\equiv (\neg p \vee \neg q) \vee (p \vee q)$	<b>De Morgan</b>
$\equiv \neg p \vee \neg q \vee p \vee q$	<b>Associative law</b>
$\equiv (\neg p \vee p) \vee (\neg q \vee q)$	<b>Associative law</b>
$\equiv T \vee T$	<b>Negation laws</b>
$\equiv T$	<b>Domination law</b>

**This is proof!**  
**Algebraic transformations**

# Quantifiers

---

---

**Universe of discourse:** The collection of values that a variable can take

**Universal quantifier,  $\forall$ :**  $\forall xP(x)$ , “for all  $x$   $P(x)$ ”  
“ $P(x)$  is T for all values of  $x$  in the universe of discourse”

(Example) Universe of discourse consists of all integers

$\forall x(x + 1 > x)$  is T

$\forall x(x^2 > x)$  is F ( $P(0)$  is F, **counterexample**)

**Existential quantification,  $\exists$ :**  $\exists xP(x)$ , “there is an  $x$  such that  $P(x)$ ”  
“There exists an element  $x$  in the universe of discourse such that  $P(x)$  is T”

(Example) Universe of discourse consists of all integers

$\exists x(x > 3)$  is T ( $P(4)$  is T for example)

# Negating Quantifiers

---

---

$$\neg \forall x P(x) \equiv \exists x \neg P(x)$$

“it is not the case that  $P(x)$  is T for all  $x$ ”

$\equiv$  “there exists  $x$  such that  $P(x)$  is F”

(Example) Negation of “all Americans eat cheeseburgers”

“there is an American who do not eat cheeseburgers”

$$\neg \exists x P(x) \equiv \forall x \neg P(x)$$

“it is not the case that there exists  $x$  such that  $P(x)$  is T”

$\equiv$  “ $P(x)$  is F for all  $x$ ”

(Example) Negation of “there is an honest politician”

“all politicians are dishonest”

These equivalences are just De Morgan’s theorems:

- $\neg(P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n)) \equiv \neg P(x_1) \vee \neg P(x_2) \vee \dots \vee \neg P(x_n)$
- $\neg(P(x_1) \vee P(x_2) \vee \dots \vee P(x_n)) \equiv \neg P(x_1) \wedge \neg P(x_2) \wedge \dots \wedge \neg P(x_n)$

# Nesting Quantifiers

---

---

1.  $\forall x \forall y P(x,y)$ : “ $P(x,y)$  is T for every pair  $x,y$ ”
2.  $\exists x \exists y P(x,y)$ : “there is a pair for which  $P(x,y)$  is T”
3.  $\forall x \exists y P(x,y)$ : “for every  $x$  there is a  $y$  for which  $P(x,y)$  is T”
4.  $\exists x \forall y P(x,y)$ : “there is a  $x$ , for which  $P(x,y)$  is T for all  $y$ ”

(Example)  $P(x, y) =$  “ $x$  relies upon  $y$ ”

$\forall x (\exists y P(x,y))$ : “everyone has someone to rely on”

$\exists x (\forall y P(x,y))$ : “there is a needy person who relies on everybody”

# Proof

---

---

**Axioms:** Statements assumed to be T, defining a mathematical structure

**Theorem:** A statement that can be shown to be T

**Proof:** Demonstration that a theorem is T

**Rules of inference:** Patterns to deduce a true statement (**conclusion**) from a set of other true statements (**hypotheses**)

**General form:** If we know that a set of hypotheses are all T, then a conclusion is T

hypothesis 1 ( $h_1$ )

hypothesis 2 ( $h_2$ )

...

∴ (denotes “therefore”) conclusion ( $c$ )

**Associated tautology:**  $h_1 \wedge h_2 \wedge \dots \rightarrow c$

# Examples of Axioms

---

---

## Axioms of Euclidean geometry (~300BC)

1. Given two distinct points, one can draw one and only one line segment connecting these points.
2. Given two distinct points, one can draw one and only one circle centered at the first point and passing through the second one.
3. Any two right angles are equal.
4. Every line segment can be infinitely continued in either direction.
5. For any given line  $l$  and a point  $P$  not on that line one can draw one and only one line  $l_1$  through  $P$  that will not intersect the original line  $l$ .

## Axioms of Riemann's geometry (1854)

Euclid's axioms 1-4

- 5'. Given a straight line and a point not on the line, there are no straight lines through the point parallel to the original line.

## Axioms in Newtonian mechanics

1. An object at rest tends to stay at rest and an object in motion tends to stay in motion with the same speed and in the same direction unless acted upon by an unbalanced force.
2. The acceleration of an object as produced by a net force is directly proportional to the magnitude of the net force, in the same direction as the net force, and inversely proportional to the mass of the object.
3. For every action, there is an equal and opposite reaction.



# Rules of Inference

Rule of Inference	Tautology	Name
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p}{q} \frac{q}{\therefore p \wedge q}$	$(p) \wedge (q) \rightarrow p \wedge q$	Conjunction
$\frac{p}{p \rightarrow q} \frac{p \rightarrow q}{\therefore q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\frac{\neg q}{p \rightarrow q} \frac{p \rightarrow q}{\therefore \neg p}$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens

# Rules of Inference

---

---

Rule of Inference	Tautology	Name
$\begin{array}{l} p \rightarrow q \\ \underline{q \rightarrow r} \\ \therefore p \rightarrow r \end{array}$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	<b>Hypothetical syllogism</b>
$\begin{array}{l} p \vee q \\ \underline{\neg p} \\ \therefore q \end{array}$	$[(p \vee q) \wedge \neg p] \rightarrow q$	<b>Disjunctive syllogism</b>
$\begin{array}{l} p \vee q \\ \underline{\neg p \vee r} \\ \therefore q \vee r \end{array}$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	<b>Resolution</b>

# Rules of Inference for Quantified Statements

---

---

Rule of Inference	Name
$\frac{\forall xP(x)}{\therefore P(c) \text{ for a particular } c}$	Universal instantiation
$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall xP(x)}$	Universal generalization
$\frac{\exists xP(x)}{\therefore P(c) \text{ for some } c}$	Existential instantiation
$\frac{P(c) \text{ for some } c}{\therefore \exists xP(x)}$	Existential generalization

# Methods of Proving Theorems

---

---

Proving implications  $p \rightarrow q$ :

**Direct proof:** Assume  $p$  is T, and use rules of inference to prove that  $q$  is T

**Indirect proof:** Prove its contrapositive; assume  $\neg q$ , and prove  $\neg p$

**Proof by cases:** Prove  $(p_1 \vee p_2) \rightarrow q$  by proving  $(p_1 \rightarrow q)$  and  $(p_2 \rightarrow q)$


- Based on  $[(p_1 \vee p_2) \rightarrow q] \equiv [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q)]$

# Sample Direct Proof

---

---

Give a direct proof of the theorem “If  $n$  is an odd integer, then  $n^2$  is an odd integer.”

*Solution:* Assume that the hypothesis of this implication is true, namely, suppose that  $n$  is odd. Then  $n = 2k + 1$ , where  $k$  is an integer. It follows that  $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ . Therefore,  $n^2$  is an odd integer (it is one more than twice an integer). 

**Write your answer to a homework at this  
level of readability!**

# Proof by Contradiction

---

## Proving $p$ :

- Prove  $\neg p \rightarrow (q \wedge \neg q)$
- Since  $(q \wedge \neg q) \equiv \text{F}$  (contradiction, by negation law),  $\neg p \rightarrow \text{F}$
- This is only T, if  $\neg p = \text{F}$  (i.e.,  $p = \text{T}$ )

## (Example) Prove that $p$ : “ $\sqrt{2}$ is irrational”

- Assume  $\neg p$ : “ $\sqrt{2}$  is rational (i.e.,  $\sqrt{2} = a/b$ , where integers  $a$  &  $b$  have no common factors)”.
- It follows that  $2 = a^2/b^2$ , hence  $2b^2 = a^2$ . This means  $a^2$  is even, which implies  $a$  is even. Furthermore, since  $a$  is even,  $a = 2c$  for some integer  $c$ . Thus  $2b^2 = 4c^2$ , so  $b^2 = 2c^2$ . This means  $b^2$  is even, which implies  $b$  is even.
- It has been shown that  $\neg p \rightarrow$  “ $\sqrt{2} = a/b$ , where integers  $a$  &  $b$  have no common factors”  $\wedge$  “2 divides both  $a$  &  $b$ ”.

# Existence Proofs

---

---

**Existence proof: Proving  $\exists xP(x)$**

- **Constructive proof:** Find an element  $a$  such that  $P(a)$  is T
- **Nonconstructive proof:** For example, proof by contradiction — prove that its negation leads to contradiction