IDMA 2024 : WEEK 3

MATHEMATICAL LOGIC & PROOFS

SRIKANTH SRINIVASAN

Mathematical Logic

→ Formalizing logical statements & arguments.

Mathematical Logic

→ Formalizing logical statements & arguments.

"If it is raining, then the asphalt is wet."

"If CO_2 concentrations rise, then the temperature rises."

"If a number is even, then it is the sum of two primes".

"If the input graph is connected, then the algorithm finds a path between any two nodes."

Why?

Why?

→ Natural language is sometimes ambi-guous leading to confusions & often mistakes.

Why?

→ Natural language is sometimes ambi-guous leading to confusions & often mistakes.

Logical syntax allows us to be precise, distinguish correct from wrong arguments easily.

Why?

→ Natural language is sometimes ambi-guous leading to confusions & often mistakes.

Logical syntax allows us to be precise, distinguish correct from wrong arguments easily.

→ Automated reasoning

Set-Up

Propositional logic

Set-Up

Propositional logic

Propositions - Statements that can be either true or false

→ $x > 2$.

→ It is raining.

→ Go outside.

Set-Up

Propositional logic

Propositions - Statements that can be either true or false

→ $x > 2$ ✓

→ It is raining. ✓

→ Go outside. ✗ - not a proposition.

Set-Up

Propositional logic

Propositions - Statements that can be either true or false

→ $x > 2$ ✓

→ It is raining. ✓

→ Go outside. ✗ - not a proposition.

p, q, r - denote propositions.

SET-Up (Contd.) - Compound statements / Propositional formulas

↳ Combine propositions with connectives.

SET-Up (Contd.) - Compound statements / Propositional formulas

↳ Combine propositions with connectives.

$\sim$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$
NOT	AND	OR	IMPLY	EQUIVALENT

SET-Up (Contd.) - Compound statements / Propositional formulas

↳ Combine propositions with connectives.

$\sim$ $\wedge$ $\vee$ $\rightarrow$ $\leftrightarrow$

NOT AND OR IMPLY EQUIVALENT

$\sim p$ - Statement is true when p is false & false when p is true.

($\neg p$)

p	$\sim p$
T	F
F	T

SET-Up (Contd.) - Compound statements / Propositional formulas

↳ Combine propositions with connectives.

$\sim$ $\wedge$ $\vee$ $\rightarrow$ $\leftrightarrow$

NOT AND OR IMPLY EQUIVALENT

$\sim p$ - Statement is true when p is false & false when p is true.

($\neg p$)

p	$\sim p$
T	F
F	T

} Truth table of NOT

AND & OR

p, q

$p \wedge q$ - "p AND q"

$p \vee q$ - "p OR q"

AND & OR

p, q

$p \vee q$ - "p OR q"

$p \wedge q$ - "p AND q"

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

AND & OR

p, q

$p \wedge q$ - "p AND q"

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

$p \vee q$ - "p OR q"

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

AND & OR

p, q

$p \wedge q$ - "p AND q"

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

$p \vee q$ - "p OR q"

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

OBS: OR is ambiguous in natural language!

"Mary is a singer or a poet."

AND & OR

p, q

$p \wedge q$ - "p AND q"

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

$p \vee q$ - "p OR q"

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

OBS: OR is ambiguous in natural language!

"Mary is a singer or a poet."

IMPLICATION

AND, OR, NOT - enough to construct any compound statement.

Yet, for ease of use, we have others..

IMPLICATION

AND, OR, NOT - enough to construct any compound statement.

Yet, for ease of use, we have others..

$p \rightarrow q$ - p IMPLIES q

$(p \Rightarrow q)$

IMPLICATION

AND, OR, NOT - enough to construct any compound statement.

Yet, for ease of use, we have others..

$p \rightarrow q$ - p IMPLIES q

$(p \Rightarrow q)$

p - Hypothesis

q - Conclusion

"If you have a million dollars, you are happy."

IMPLICATION

AND, OR, NOT - enough to construct any compound statement.

Yet, for ease of use, we have others..

$p \rightarrow q$ - p IMPLIES q

$(p \Rightarrow q)$

p - Hypothesis
q - Conclusion

"If you have a million dollars, you are happy."

p	q	p → q
F	F	
F	T	
T	F	
T	T	

IMPLICATION

AND, OR, NOT - enough to construct any compound statement.

Yet, for ease of use, we have others..

$p \rightarrow q$ - p IMPLIES q

$(p \Rightarrow q)$

p - Hypothesis
q - Conclusion

"If you have a million dollars, you are happy."

p	q	$p \Rightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

IMPLICATION

AND, OR, NOT - enough to construct any compound statement.

Yet, for ease of use, we have others..

$p \rightarrow q$ - p IMPLIES q

($p \Rightarrow q$)

p - Hypothesis

q - Conclusion

"If you have a million dollars, you are happy."

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

Same as $(\sim p) \vee q$

IMPLICATION

$p \to q$ not the same as $q \to p$ (CONVERSE)

IMPLICATION

$p \to q$ not the same as $q \to p$ (CONVERSE)

is the same as $\sim q \to \sim p$ (CONTRAPOSITIVE)

IMPLICATION

$p \to q$ not the same as $q \to p$ (CONVERSE)

is the same as $\sim q \to \sim p$ (CONTRAPOSITIVE)

$p \to q$: "If you have a million dollars, you are happy."

$q \to p$: "If you are happy, you have a million dollars."

$\sim q \to \sim p$: "If you are not happy, you don't have a million dollars."

IMPLICATION

$p \to q$ not the same as $q \to p$ (CONVERSE)

is the same as $\sim q \to \sim p$ (CONTRAPOSITIVE)

$p \to q$: "If you have a million dollars, you are happy."

$q \to p$: "If you are happy, you have a million dollars."

$\sim q \to \sim p$: "If you are not happy, you don't have a million dollars."

p	q	$p \to q$	$q \to p$	$\sim q \to \sim p$
F	F	T	T	T
F	T	T	F	T
T	F	F	T	F
T	T	T	T	T

IMPLICATION

$p \to q$ not the same as $q \to p$ (CONVERSE)

is the same as $\sim q \to \sim p$ (CONTRAPOSITIVE)

$p \to q$: "If you have a million dollars, you are happy."

$q \to p$: "If you are happy, you have a million dollars."

$\sim q \to \sim p$: "If you are not happy, you don't have a million dollars."

p	q	$p \to q$	$q \to p$	$\sim q \to \sim p$
F	F	T	T	T
F	T	T	F	T
T	F	F	T	F
T	T	T	T	T

$(p \to q) \equiv (\sim q \to \sim p)$

↓

"the same as"

not part of our logical syntax.

Time for a little quiz!

EQUIVALENCE

$p \leftrightarrow q$ - "p if and only if q"

EQUIVALENCE

$p \leftrightarrow q$ - "p if and only if q"

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

EQUIVALENCE

$p \leftrightarrow q$ - "p if and only if q"

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

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

More Complicated formulas

$$\Big(\big((p \to q) \leftrightarrow r\big) \vee (\sim p)\Big) \wedge \big((q \to (\sim r)) \wedge s\big)$$

More Complicated formulas

$$\Big(\big((p \to q) \leftrightarrow r\big) \vee (\sim p)\Big) \wedge \big((q \to (\sim r)) \wedge s\big)$$

How many rows in the truth table?

More Complicated formulas

$$\Big(\big((p \to q) \leftrightarrow r\big) \vee (\sim p)\Big) \wedge \big((q \to (\sim r)) \wedge s\big)$$

How many rows in the truth table?

Formula with n variables - 2^n.

BASIC PROPERTIES OF AND, OR, NOT

(1)	$p \vee q$	$\equiv$	$q \vee p$	} COMMUTATIVITY
(2)	$p \wedge q$	$\equiv$	$q \wedge p$	
(3)	$p \vee (q \vee r)$	$\equiv$	$(p \vee q) \vee r$	} ASSOCIATIVITY
(4)	$p \wedge (q \wedge r)$	$\equiv$	$(p \wedge q) \wedge r$	
(5)	$p \vee (q \wedge r)$	$\equiv$	$(p \vee q) \wedge (p \vee r)$	} DISTRIBUTIVITY
(6)	$p \wedge (q \vee r)$	$\equiv$	$(p \wedge q) \vee (p \wedge r)$	
(7)	$\sim(\sim p)$	$\equiv$	p	LAW OF THE EXCLUDED MIDDLE
(8)	$\sim(p \vee q)$	$\equiv$	$\sim p \wedge \sim q$	} DE MORGAN'S LAWS
(9)	$\sim(p \wedge q)$	$\equiv$	$\sim p \vee \sim q$	

BASIC PROPERTIES OF IMPLICATION AND EQUIVALENCE

(a) $p \to q \equiv \sim p \vee q$

(b) $p \to q \equiv \sim q \to \sim p$

(c) $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

(d) $\sim(p \to q) \equiv p \wedge \sim q$

(e) $\sim(p \leftrightarrow q) \equiv (p \wedge \sim q) \vee (\sim p \wedge q)$

Tautologies, Contradictions & Satisfiable formulas

Tautologies, Contradictions & Satisfiable formulas

Tautology - true for any assignment to propositional variables

Eg: $S_1 \equiv S_2$: $S_1 \leftrightarrow S_2$ a tautology.

Tautologies, Contradictions & Satisfiable formulas

Tautology - true for any assignment to propositional variables

Eg: $S_1 \equiv S_2$: $S_1 \leftrightarrow S_2$ a tautology.

Contradiction - false for any assignment to propositional variables -

Eg: $p \wedge (\sim p)$

Tautologies, Contradictions & Satisfiable formulas

Tautology - true for any assignment to propositional variables

Eg: $S_1 \equiv S_2$: $S_1 \leftrightarrow S_2$ a tautology.

Contradiction - false for any assignment to propositional variables -

Eg: $p \wedge (\sim p)$

Satisfiable - true for some assignment formula

Eg: $(p \vee \sim q) \wedge (\sim p \vee q)$

Tautologies, Contradictions & Satisfiable formulas

F a

contradiction

Tautologies, Contradictions & Satisfiable formulas

F a contradiction $\equiv$ F is not satisfiable

Tautologies, Contradictions & Satisfiable formulas

$\sim F$ is a tautology $\equiv$ F a contradiction $\equiv$ F is not satisfiable

Tautologies, Contradictions & Satisfiable formulas

$\sim F$ is a tautology $\equiv$ F a contradiction $\equiv$ F is not satisfiable

Computational problem:

Input: F a propositional formula

Output: Is F a tautology / contradiction / satisfiable?

Tautologies, Contradictions & Satisfiable formulas

$\sim F$ is a tautology $\equiv$ F a contradiction $\equiv$ F is not satisfiable

Computational problem:

Input: F a propositional formula

Output: Is F a tautology / contradiction / satisfiable?

Central problem in Computer Science!

Tautologies, Contradictions & Satisfiable formulas

$\sim F$ is a tautology $\equiv$ F a contradiction $\equiv$ F is not satisfiable

Computational problem:

Input: F a propositional formula

Output: Is F a tautology / contradiction / satisfiable?

Central problem in Computer Science!

Easy algorithm using truth table: takes time $2^{\#\text{variables}}$

Tautologies, Contradictions & Satisfiable formulas

Question: Do any of these problems have a polynomial-time algorithm?

Tautologies, Contradictions & Satisfiable formulas

Question: Do any of these problems have a polynomial-time algorithm?

P vs. NP problem - Suspected answer: No.

Tautologies, Contradictions & Satisfiable formulas

Question: Do any of these problems have a polynomial-time algorithm?

P vs. NP problem - Suspected answer: No.

Question: Can we explain when this problem can be solved in practice?

Tautologies, Contradictions & Satisfiable formulas

Question: Do any of these problems have a polynomial-time algorithm?

P vs. NP problem - Suspected answer: No.

Question: Can we explain when this problem can be solved in practice?

Question: Can we efficiently verify that a formula is a contradiction/tautology?

Tautologies, Contradictions & Satisfiable formulas

Question: Do any of these problems have a polynomial-time algorithm?

P vs. NP problem - Suspected answer: No.

Question: Can we explain when this problem can be solved in practice?

Question: Can we efficiently verify that a formula is a contradiction/tautology?

NP vs. co-NP problem - Suspected answer: No.

Predicates

Formulas can talk about specific objects.

Numbers, sets, ...

Predicates

Formulas can talk about specific objects.

Numbers, sets, ...

$P(x): x^2 - 8x + 15 = 0$

Predicates

Formulas can talk about specific objects.

Numbers, sets, ...

$P(x)$: $x^2 - 8x + 15 = 0$

$Q(x,y,z)$: $(x \in \mathbb{Z}) \wedge (y \in \mathbb{Z}) \wedge (z \in \mathbb{Z}) \wedge$
$(x \geq 1) \wedge (y \geq 1) \wedge (z \geq 1) \wedge$
$(x^3 + y^3 = z^3)$

Predicates

Formulas can talk about specific objects.

Numbers, sets, ...

$P(x)$: $x^2 - 8x + 15 = 0$

$Q(x,y,z)$: $(x \in \mathbb{Z}) \wedge (y \in \mathbb{Z}) \wedge (z \in \mathbb{Z}) \wedge$
$(x \geq 1) \wedge (y \geq 1) \wedge (z \geq 1) \wedge$
$(x^3 + y^3 = z^3)$

Can use this to define sets.

$$S = \{x \in \mathbb{R} \mid P(x)\}$$

Quantified formulas

Quantified formulas

Existential quantifier

$$\exists x \in \mathbb{R} \quad x^2 - 5x + 18 = 0$$

"There exists a real x satisfying the equation $x^2 - 5x + 18 = 0$"

Quantified formulas

Existential quantifier

$$\exists x \in \mathbb{R} \quad x^2 - 5x + 18 = 0$$

"There exists a real x satisfying the equation $x^2 - 5x + 18 = 0$"

Universal quantifier:

$$\forall x \in \mathbb{R} \quad x^2 - 5x + 18 = 0$$

"All real numbers x satisfy the equation $x^2 - 5x + 18 = 0$"

Quantified formulas (contd.)

Can combine existential & universal quantifiers

Quantified formulas (contd.)

Can combine existential & universal quantifiers

$$\forall x \in \mathbb{Z} \quad \exists y \in \mathbb{Z} \quad y = x^2.$$

"For every integer x there is an integer y that is the square of x."

Quantified formulas (contd.)

Can combine existential & universal quantifiers

$$\forall x \in \mathbb{Z} \quad \exists y \in \mathbb{Z} \quad y = x^2.$$

"For every integer x there is an integer y that is the square of x."

$$\exists y \in \mathbb{Z} \quad \forall x \in \mathbb{Z} \quad y = x^2$$

"There is an integer y such that for all integers x, y is the square of x."

Quantified formulas (contd.)

Can combine existential & universal quantifiers

$$\forall x \in \mathbb{Z} \quad \exists y \in \mathbb{Z} \quad y = x^2.$$

"For every integer x there is an integer y that is the square of x."

$$\exists y \in \mathbb{Z} \quad \forall x \in \mathbb{Z} \quad y = x^2$$

"There is an integer y such that for all integers x, y is the square of x."

QUANTIFIER ORDER MATTERS!!

Negating quantifiers

$$F: \quad \exists x \in \mathbb{Z} \quad x^2 = 2$$

There exists an integer x that squares to 2.

Negating quantifiers

$$F: \quad \exists x \in \mathbb{Z} \quad x^2 = 2$$

There exists an integer x that squares to 2.

$$\sim F: \quad \forall x \in \mathbb{Z} \quad \sim (x^2 = 2)$$

Negating quantifiers

$$F: \quad \exists x \in \mathbb{Z} \quad x^2 = 2$$

There exists an integer x that squares to 2.

$$\sim F: \quad \forall x \in \mathbb{Z} \quad \sim (x^2 = 2)$$

$$\| \; \|$$

$$\forall x \in \mathbb{Z} \quad x^2 \neq 2$$

Negating quantifiers

$$F: \quad \exists x \in \mathbb{Z} \quad x^2 = 2$$

There exists an integer x that squares to 2.

$$\sim F: \quad \forall x \in \mathbb{Z} \quad \sim (x^2 = 2)$$

$$\| \|$$

$$\forall x \in \mathbb{Z} \quad x^2 \neq 2$$

$$\sim(\exists x \in S \quad P(x)) \equiv \forall x \in S \quad \sim P(x)$$

$$\sim(\forall x \in S \quad P(x)) \equiv \exists x \in S \quad \sim P(x)$$

Convention

$P(x) \to Q(x)$ (without quantifiers)

usually means

$\forall x \quad P(x) \to Q(x)$

Convention

$P(x) \to Q(x)$ (without quantifiers)

usually means

$\forall x \quad P(x) \to Q(x)$

Eg: $(x^2 = 2) \to (x \notin \mathbb{Q})$

$\forall x \in \mathbb{R} \quad (x^2 = 2) \to (x \notin \mathbb{Q})$