W3203
Discrete Mathematics

Logic and Proofs

Spring 2015
Instructor: Ilia Vovsha

http://www.cs.columbia.edu/~vovsha/w3203

Outline

- Propositional Logic
- Operators
- Truth Tables
- Logical Equivalences
- Laws of Logic
- Rules of Inference
- Quantifiers
- Proof Patterns
- Text: Rosen 1
- Text: Lehman 1-3

Logic Puzzle

- Three kinds of people live on an island:
  - *Knights (K)*: always tell the truth
  - *Knaves (V)*: always lie
  - *Spies (S)*: either lie or tell the truth
- You meet 3 people, A, B, and C
  - You know one is K, one is V, and one is S
  - Each of them knows all of their types
  - They make three statements about each other
  - Can you determine who is the knight/knave/spy?

Logic Puzzle

- Statements:
  - *A*: “I am the knight”
  - *B*: “A is not the knave”
  - *C*: “B is not the knave”
- Can you determine who is the knight/knave/spy?

Logic Puzzle (solution)

- Statements:
  - *A*: “I am the knight”
  - *B*: “A is not the knave”
  - *C*: “B is not the knave”
- Can you determine who is the knight/knave/spy?
  - Suppose A is the Knight (K). Then B tells truth, B must be a spy (S). But C tells truth, can’t be a knave (V).
  - Suppose B is **K**. Then B tells truth, A must be **S**. Hence C is **V**, but he tells truth. Hence we have a contradiction.
  - C must be **K**. Then C tells truth, B must be **S**. A is the **V**.

Propositions

- Definition: A *proposition* is a declarative sentence (statement) that is either true (T) or false (F), but not both
  - Fact-based declaration
    - 1 + 1 = 2
    - "A is not the knave"
    - "If A is a knight, then B is not a knight"
  - Excludes commands, questions and opinions
    - "What time is it?"
    - "Be quiet!"
  - What about statements with (non-constant) variables?
    - x + 2 = 5
    - "n is an even number"

Predicates

- Definition: A *predicate* is a proposition whose truth depends on one or more variables
  - Variables can have various domains:
    - nonnegative integers
    - x > 1
    - people: “all people on the island are knights, knaves or spies”
  - Notation: P(x)
    - Not an ordinary function!
    - P(x) is either True or False

Puzzle (propositions)

- Statements:
  - *A*: “I am the knight”
  - *B*: “A is not the knave”
  - *C*: “B is not the knave”
- Lets introduce propositional (*boolean*) variables:
  - V_A ::= “A is the knave”, V_B ::= “B is the knave”
  - V_A or V_B ::= “A is the knave or B is the knave”
  - If V_A then not V_B ::= “If A is the knave then B is not the knave”
  - K(p) ::= “person p is a knight”

Constructing Propositions

- English: modify, combine, and relate statements with "not", "and", "or", "implies", "if-then"
- *Atomic propositions*: boolean constant (T,F) or variable (e.g. p, q, r, V_A ,V_B)
- *Compound propositions*: apply *operators* to atomic forms in order of precedence.
  - Construct from logical connectives and other propositions.
- Precise mathematical meaning of operators can be specified by *truth tables*

Common Operators

- *Negation*: "not" ¬
- *Conjunction*: "and" ∧
- *Disjunction*: "or" ∨
- *Implication/ Conditional*: "if-then" →
- *Monadic* operator: one argument
  - Examples: identity, negation, constant ... (4 operators)
- *Dyadic* operator: two arguments
  - Examples: conjunction, disjunction ... (16 operators)

Truth Tables (idea)

- Boolean values & domain: {T,F}
- *n-tuple*: $(x_1, x_2, \ldots, x_n)$
- Operator on n-tuples : $g(x_1 = v_1, x_2 = v_2, \ldots, x_n = v_n)$
- Definition: A *truth table* defines an operator 'g' on n-tuples by specifying a boolean value for each tuple
- Number of rows in a truth table?
  - $R = 2^n$
- Number of operators with n arguments?
  - 2^R

Truth Table (negation)

- The *negation* of a proposition p is denoted by $\neg p$ and has this truth table:

p	$\neg p$
T	F
F	T

- **Example**: If p denotes "The earth is round.", then $\neg p$ denotes "It is not the case that the earth is round," or more simply "The earth is not round."

Truth Table (conjunction)

- The *conjunction* of propositions p and q is denoted by $p \land q$ and has this truth table:

p	q	$p \land q$
T	T	T
T	F	F
F	T	F
F	F	F

- **Example**: If p denotes “I am at home.” and q denotes “It is raining.” then $p \land q$ denotes “I am at home and it is raining.”

Truth Table (disjunction)

- The *disjunction* of propositions p and q is denoted by $p \lor q$ and has this truth table

p	q	$p \lor q$
T	T	T
T	F	T
F	T	T
F	F	F

- **Example**: If p denotes "I am at home." and q denotes "It is raining." then $p \lor q$ denotes "I am at home or it is raining."

Truth Table (exclusive or)

- If only one of the propositions p and q is true but NOT both, we use "Xor" symbol

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

- **Example**: When reading the sentence "Soup or salad comes with this entrée," we do not expect to be able to get both soup and salad

Truth Table (implication)

- If p and q are propositions, then $p \rightarrow q$ is a *conditional statement* or *implication:* "if p, then q"

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

- **Example**: If p denotes "I am at home." and q denotes "It is raining." then $p \rightarrow q$ denotes "If I am at home then it is raining."
- In $p \rightarrow q$, p is the *antecedent* and q is the *consequent*

Understanding Implication

- There does not need to be any connection between the antecedent or the consequent.
  - The "meaning" of $p \to q$ depends only on the truth values of p and q.
  - "If pigs fly then you are rich."
- Think of an obligation or a contract
  - "If I am elected, then I will lower taxes."

Puzzle (compound propositions)

- Statements:
  - *A*: "I am the knight"
  - *B*: "A is not the knave"
  - *C*: "B is not the knave"
- Compound propositions:
  - $\neg V_A$ ::= "A is not the knave"
  - $K_A \vee K_B$ ::= "A is the knight or B is the knight"
  - $V_A \rightarrow \neg V_B$ ::= "If A is the knave, then B is not the knave"
  - $K_c \rightarrow \neg V_B$ ::= "If C is the knight, then C tells the truth"

Truth Table (rules)

- Row for every combination of values for atomic propositions
- Column for truth value of each expression in the compound proposition
- Column (far right) for the truth value of the compound proposition
- Build step by step
  - $p \vee q \rightarrow \neg r$ means $(p \vee q) \rightarrow \neg r$
- Big problem with this approach!

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

Truth Table (example)

- Construct a truth table for $p \lor q \to \neg r$

p	q	r	¬r	p ∨ q	p ∨ q → ¬r
T	T	T	F	T	F
T	T	F	T	T	T
T	F	T	F	T	F
T	F	F	T	T	T
F	T	T	F	T	F
F	T	F	T	T	T
F	F	T	F	F	T
F	F	F	T	F	T

Logical Equivalences

- Two compound propositions *p* and *q* are *logically equivalent* if and only if the columns in the truth table giving their truth values agree.
  - We write this as $p \Leftrightarrow q$ or as $p \equiv q$
  - Not an operator! (relation on propositions)
- This truth table shows $\neg p \vee q$ is equivalent to $p \rightarrow q$

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

Converse, Contrapositive, & Inverse

- Given $p \rightarrow q$,
- The *converse* is: $q \rightarrow p$
- The *contrapositive* is: $\neg q \rightarrow \neg p$
- The *inverse* is: $\neg p \rightarrow \neg q$
- Example: "Raining is a sufficient condition for my not going to town."
  - Converse: If I do not go to town, then it is raining.
  - Inverse: If it is not raining, then I will go to town.
  - Contrapositive: If I go to town, then it is not raining.

Truth Table (biconditional)

- If p and q are propositions, then $p \leftrightarrow q$ is a *biconditional (IFF)* statement: "p if and only if q"

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

- **Example**: If p denotes "I am at home." and q denotes "It is raining." then $p \leftrightarrow q$ denotes "I am at home if and only if it is raining."

Terminology ($p \rightarrow q$)

- Simple English:
  - **if** p**, then** q — p **implies** q
  - **if** p, q — p **only if** q
  - q **unless** $\neg p$ — q **when** p
  - q **if** p
  - q **whenever** p — p **is sufficient for** q
  - q **follows from** p — q **is necessary for** p
- A necessary condition for p is q
- A sufficient condition for q is p
- Biconditional:
  - p is necessary and sufficient for q
  - p *iff* q

Tautology & Contradiction

- *Tautology* is a proposition which is always true
  - Example: $p \lor \neg p$
- *Contradiction* is a proposition which is always false
  - Example: $p \land \neg p$
- *Contingency* is a proposition which is neither a tautology or a contradiction

P	$\neg p$	$p \lor \neg p$	$p \land \neg p$
T	F	T	F
F	T	T	F

Laws of Logic

- Trivial laws: identity, double negation
- Express $\wedge$ and $\vee$ in terms of each other via $\neg$

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

- Order & Parenthesis (3,4):

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

$$p \wedge q \equiv q \wedge p$$

- Distribute operator (5):

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

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

- Laws involving (bi)conditional operators

The Axiomatic Method

- Begin with some assumptions (*axioms*)
  - Given as true or used to specify the system
- Provide an argument (*proof)*
  - Sequence (chain) of *logical deductions* and previous "results" (*premises*)
  - Ends with the proposition in question (*conclusion*)
- Important true propositions are called *theorems*
- Hierarchy of derived truths:
  - *Proposition*: minor result (theorem)
  - *Lemma*: preliminary proposition useful for proving later propositions
  - *Corollary*: a proposition that follows in just a few logical steps from a theorem

Logical Argument

- To provide a logical argument (*proof*):
  - Sequence of *logical deductions* (rules of inference) and previous compound propositions (*premises*)
  - Ends with the proposition in question (*conclusion*)
- A *valid* argument can never leads to incorrect (false) conclusion from correct statements (premises)
- *Fallacy*: from true statements to incorrect conclusion
- If some premises untrue: conclusion of valid argument might be false
- Conclusion of fallacy might be true
- If premises are correct & argument is valid, conclusion is correct

Rules of Inference (modus ponens)

- Example:
  - Let *p* be "It is snowing."
  - Let *q* be "I will study discrete math."

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

  - "If it is snowing, then I will study discrete math."
  - "It is snowing."
  - "Therefore , I will study discrete math."

- Method of rule validation: record (in a truth table) where all premises are true. If the conclusion is also true in every case, then the rule is valid

Rules of Inference (fallacy)

- Affirm the consequent, conclude the antecedent
- Example:
  - Let *p* be "It is snowing."
  - Let *q* be "I will study discrete math."

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

$$p$$

  - "If it is snowing, then I will study discrete math."
  - "I will study discrete math."
  - "Therefore, it is snowing."

Rules of Inference (modus tollens)

- Example:
  - Let *p* be "It is snowing."
  - Let *q* be "I will study discrete math."

$$\begin{array}{l} p \rightarrow q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

  - "If it is snowing, then I will study discrete math."
  - "I will not study discrete math."
  - "Therefore, it is not snowing."

- Fallacy: deny the antecedent (p), conclude the consequent (q) is false

Common Rules

- Addition: $$\frac{p}{\therefore p \vee q}$$
- Simplification: $$\frac{p \wedge q}{\therefore q}$$
- Disjunctive-syllogism: $$\frac{\begin{array}{c} p \vee q \\ \neg p \end{array}}{\therefore q}$$
- Hypothetical-syllogism: $$\frac{\begin{array}{c} p \rightarrow q \\ q \rightarrow r \end{array}}{\therefore p \rightarrow r}$$

Puzzle (logical argument)

- Statements:
  - *A*: "I am the knight" K_A
  - *B*: "A is not the knave" $\neg V_A$
  - *C*: "B is not the knave" $\neg V_B$
- Argument:
  - Suppose A is the Knight (K). Then B tells truth, B must be a spy (S). But C tells truth, can't be a knave (V)

  - $K_A \rightarrow \neg V_A$ ::= "If A is the knight, then A is not the knave"
  - $\neg V_A \rightarrow (K_B \vee S_B)$ ::= "If A is not knave, then B is knight or spy"
  - $\neg V_B \rightarrow (K_c \vee S_c)$ ::= "If B is not knave, then C is knight or spy"
  - $S_B \rightarrow \neg(S_A \vee S_c)$ ::= "If B is the spy then A and C are not spies"

Quantifiers

- Purpose: express words such as "all", "some"
- *Universal Quantifier*: "For all", $\forall$
- *Existential Quantifier*: "There exists", $\exists$
- Definition:
  - $\forall x\ P(x)$ asserts P(x) is true for <u>every</u> x in the domain
  - $\exists x\ P(x)$ asserts P(x) is true for <u>some</u> x in the domain

Quantifiers (examples)

- $\forall x\, P(x)$: "For all x, P(x)" or "For every x, P(x)"
- $\exists x\, P(x)$: "For some x, P(x)" or "There is an x such that P(x)" or "For at least one x, P(x)."
- Example:
  1) P(x) denotes "x > 0"
  2) Q(x) denotes "x is even"

  - For positive integers domain, '$\forall x\, P(x)$' is true '$\exists x\, P(x)$' is true
  - For integers domain, '$\forall x\, P(x)$' is false but '$\exists x\, P(x)$' is true
  - For integers domain, '$\forall x\, Q(x)$' is false but '$\exists x\, P(x)$' is true

Quantifiers (scope)

- Rules:
  - The quantifiers ∀ and ∃ have higher precedence than all the logical operators.
  - Note location of parenthesis:
    - $\forall x\, P(x) \vee Q(x)$ means $(\forall x\, P(x)) \vee Q(x)$
    - $\forall x\, (P(x) \vee Q(x))$ means something different
  - Variable not within scope (clause to which it applies) of any quantifier: *unbound variable*
    - $x + 4 > 2$
    - $\forall y\, [2x + 3y = 7]$

Quantifiers (translation)

- Example:
  1) P(x): “x has taken calculus.”
  2) Domain: students in class
  3) $\forall x\, P(x)$: “Every student in class has taken calculus.”

  Translate: “It is not the case that every student in class has taken calculus.”

  Answer:

  1) $\neg\forall x\, P(x)$ $\neg(\forall x)[P(x)]$
  2) “There is a student in class who has not taken calculus”

     $\exists x\, \neg P(x)$

Quantifiers (negation rules)

- Rules:

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

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

Quantifiers (translation)

- Example:
  1. "All lions are fierce."
  2. "Some lions do not drink coffee."
  3. "Some fierce creatures do not drink coffee."

  Translate to predicates:

  a. P(x): "x is a lion"
  b. Q(x): "x is fierce"
  c. R(x): "x drinks coffee"

  1. $\forall x\, [\, P(x) \rightarrow Q(x)\,]$
  2. $\exists x\, [\, P(x) \wedge \neg R(x)\,]$
  3. $\exists x\, [\, Q(x) \wedge \neg R(x)\,]$

Quantifiers (mixing)

- Nested quantifiers:
  - "Every real number has an inverse"
  - $\forall x \, \exists y \, (x + y = 0)$
  - Specify domain when not evident: the domains of x and y are the real numbers

    $$(\forall x \in \Re)(\exists y \in \Re)[x + y = 0]$$
- Does order matter?
  - Switching order is not safe when the quantifiers are different!
  - $\forall x \forall y \, P(x,y)$ and $\forall y \forall x \, P(x,y)$ have the same truth value

Nested Quantifiers (translation)

- Example 1: "Brothers are siblings."
  - **Solution**: $\forall x \, \forall y \, [\, B(x,y) \rightarrow S(x,y) \,]$
- Example 2: "Everybody loves somebody."
  - **Solution**: $\forall x \, \exists y \, L(x,y)$
- Example 3: "There is someone who is loved by everyone."
  - **Solution**: $\exists y \, \forall x \, L(x,y)$

Nested Quantifiers (negation)

- Example 1: "There does not exist a woman who has taken a flight on every airline in the world."
  - ➢ **Solution**: $\neg\exists w \forall a \exists f\ [\ P(w,f) \land Q(f,a)\ ]$
- Use negation rules to move $\neg$ as far inwards as possible:

Nested Quantifiers (negation)

- Example 1: "There does not exist a woman who has taken a flight on every airline in the world."
  - **Solution**: $\neg \exists w \forall a \exists f \, [\, P(w,f) \land Q(f,a) \,]$

- Use negation rules to move ¬ as far inwards as possible:
  - **Solution**:

$\neg \exists w \; (\forall a \, \exists f \; [\, P(w,f\,) \land Q(f,a) \,] \,)$

$\forall w \, \neg \, (\forall a \, \exists f \; [\, P(w,f\,) \land Q(f,a) \,] \,)$

$\forall w \, \exists a \, \neg \, (\exists f \; [\, P(w,f\,) \land Q(f,a) \,] \,)$

$\forall w \, \exists a \, \forall f \, \neg \, [\, P(w,f\,) \land Q(f,a) \,]$

$\forall w \, \exists a \, \forall f \;\; [\neg \, P(w,f\,) \lor \neg \, Q(f,a) \,]$

Proof Patterns

- Proof approach:
  - Direct / Indirect methods
  - Forward / Backward reasoning
- Standard templates:
  - Implication (If P then Q)
    - Contrapositive (if not Q then not P)
  - If and only if statement (P if and only if Q)
  - By cases
  - By contradiction

"Backward" Reasoning

- Claim: "arithmetic/geometric means inequality"
- Approach:
  1. Start from conclusion
  2. Show when conclusion is true
  3. Algebraic manipulation
     a. Simplify
  4. Derive simple equivalent premise which is clearly true

$$Let\ a, b > 0,\ a \neq b.$$

$$Then,\ \frac{(a+b)}{2} > \sqrt{ab}$$

$$(a+b) > 2\sqrt{ab}$$

$$(a+b)^2 > 4ab$$

$$a^2 + 2ab + b^2 > 4ab$$

$$a^2 - 2ab + b^2 > 0$$

$$(a-b)^2 > 0$$

Proving the Contrapositive

- Claim: "If r is an irrational number then √r is an irrational number"

$$Q \equiv \left\{ \frac{p}{q} :\ p, q \in Z, q \neq 0 \right\}$$

- Approach:
  1. Assume √r is rational, show that r is rational.
  2. Use definition to express √r as a fraction
  3. Algebraic manipulation: square both sides
  4. Conclude claim

Proving If and Only If

- Claim: "The standard deviation (std) of a set of numbers is zero if and only if (iff) all the values are equal to the mean"
- Approach:
  1. Construct chain of iff statements
  2. Use definition of std and mean
  3. Algebraic manipulation
     a. Simplify: square both sides
  4. Show that condition holds for each value iff condition holds for the set

Proof by Cases

- Claim: “Let x be any integer, then $x^2 + x$ is even”
- Approach:
  1. Break into cases:
     a. Case 1: x is even
     b. Case 2: x is odd
  2. Use definition of even/odd integer to express $x^2 + x$ as an even integer
     a. Case 1: $x = 2n$
     b. Case 2: $x = 2n + 1$

Proof by Contradiction

- Claim: "√2 is irrational" $\sqrt{2} \notin Q$
- Approach:
  1. Assume √2 is rational
  2. Use definition to express √2 as fraction in lowest terms
  3. Algebraic manipulation
     a. Square both sides
     b. Apply rules of divisibility
  4. Derive a negation of one of the premises (2), that is the contradiction.