Logic

Part I:

Propositional Calculus

Statements

Undefined Terms

- True, T, #t, 1
- False, F, #f, 0
- Statement, Proposition

Statement/Proposition -- Informal Definition

- S<u>tatement</u> = anything that can <u>meaningfully</u> be assigned a value of True or False
- Propositional Calculus = Study of Statements / Propositions

Examples

- "1 + 1 = 2" (Yes)
- "2 + 2 = 3" (Yes)
- "To be or not to be" (No)
- "This sentence is false." (No)
- "x > 5" (No)

Formulas

Formula

- A formula is a statement with free (unquantified) variables.
- A statement is a formula with no free (unquantified) variables.

Analogy to Scheme

- Statement ~ expression with type Boolean
- Formula ~ (Lambda ( ) Boolean expression)

Operators

Examples

• And	$p \wedge q$	(pq)
• Or	$p \vee q$	$(p+q)$
• Not	$\sim p$	($-p$ or pbar)
• Implies	$p \rightarrow q$	$(p \Rightarrow q)$
• Iff	$p \leftrightarrow q$	$(p \Leftrightarrow q)$

Observations

- Propositional Calculus is the Calculus of Operators.
- Operators have the usual informal meanings.
- Formal meanings are provided by Truth tables.

Truth Tables

Examples

p	q	$p \wedge q$	$p \vee q$	$\sim p$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	F	T	T
T	F	F	T	F	F	F
F	T	F	T	T	T	F
F	F	F	F	T	T	T

Conventions

- Or is inclusive: *p* or *q* or both
- XOR is exclusive: *p* or *q*, but not both -- $p \oplus q$
- $p \rightarrow q$ is True whenever *p* is False
- $p \rightarrow q$ is False only when *p* is True and *q* is False
- EXAMPLES

More Operators

NAND, NOR, XOR

p	q	$\sim(p \wedge q)$	$\sim(p \vee q)$	$p \oplus q$
T	T	F	F	F
T	F	T	F	T
F	T	T	F	T
F	F	T	T	F

Observations

- There are 16 possible boolean operators on two parameters.
- Every one can be written solely in terms of NAND or NOR.

Bit Operations

Idea

-- Replace *T* and *F* by 1 and 0

Examples

--	11011011001
--	10101100100
AND	10001000010
OR	11111111101
XOR	01110111101

Propositions

Proposition -- Recursive Definition

- Base Case: $p, q, r, \ldots$
- $p \wedge q,\ p \vee q,\ \sim p,\ p \rightarrow q,\ p \leftrightarrow q$

Parsing

- The inductive definition defines a tree.
- Parsing provided by the tree
- Parentheses needed for linear -- infix notation

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

Types of Propositions

Tautology

- a proposition that is always True
- all rows in the Truth Table are true
- $p \vee \sim p$

Contradiction

- a proposition that is always False
- all rows in the Truth Table are false
- $p \wedge \sim p$

Contingency

- a proposition that is neither a tautology nor a contradiction
- some rows in the Truth Table are True and some are rows are False
- $p \vee q$

<u>Logical Equivalence</u>

Definition

- *p* and *q* are logically equivalent if all rows in their Truth Table are the same.

Notation

- $p \equiv q$

Example

- $(\sim p) \vee q \equiv p \to q$ (Check Truth Table)

Remark

- $p \equiv q$ iff $p \leftrightarrow q$ is a tautology

Applications

- Proofs
- Computer Hardware -- Circuit Design

Implications

Proposition	*Converse*	*Inverse*	*Contrapositive*
$p \rightarrow q$	$q \rightarrow p$	$\sim p \rightarrow \sim q$	$\sim q \rightarrow \sim p$

Observations

- A proposition is equivalent to its contrapositive.
  - $p \rightarrow q \equiv \sim q \rightarrow \sim p$
- A proposition is NOT equivalent to its converse or inverse.
  - Examples
  - Truth Tables

Logical Equivalences (Boolean Algebra)

1. *Identity*

   $p \wedge T \equiv p$

   $p \vee F \equiv p$

2. *Domination*

   $p \vee T \equiv T$

   $p \wedge F \equiv F$

3. *Idempotence*

   $p \vee p \equiv p$

   $p \wedge p \equiv p$

4. *Double Negation*

   $\sim\sim p \equiv p$

More Logical Equivalences (Boolean Algebra)

5. *Commutative*

   $p \vee q \equiv q \vee p$

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

6. *Associative*

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

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

7. *Distributive*

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

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

De Morgan's Laws

De Morgan Laws

$$\sim (p \wedge q) = (\sim p) \vee (\sim q)$$

$$\sim (p \vee q) = (\sim p) \wedge (\sim q)$$

Proofs by Truth Tables.

Generalizes to more operators by Induction.

$$\sim (p_1 \wedge \cdots \wedge p_n) = (\sim p_1) \vee \cdots \vee (\sim p_n)$$

$$\sim (p_1 \vee \cdots \vee p_n) = (\sim p_1) \wedge \cdots \wedge (\sim p_n)$$

Axiomatic Approach to Propositional Calculus

3 *Axioms*

1. $P \to (Q \to P)$
2. $\big(P \to (Q \to R)\big) \to \big((P \to Q) \to (P \to R)\big)$
3. $\big(\sim P \to \sim Q\big) \to \big((\sim P \to Q) \to P\big)$

1 *Rule of Inference*

- Prove: P and $P \to Q$
- Conclude: Q

2 Metatheorems

- *Consistency:* All the Theorems of Propositional Calculus are Tautologies.
- *Completeness:* All Tautologies are Theorems of the Propositional Calculus.

Axiomatic Approach to Arithmetic

Axioms of Natural Numbers

1. 1 is a Natural Number.
2. If n is a natural number, then $n+1$ is a natural number.
3. Every natural number m except 1 is of the form $m = n + 1$.
4. Every nonempty subset of the natural numbers has a smallest element.
5. Axioms for addition and multiplication.

1 *Rule of Inference*

- Prove: P and $P \rightarrow Q$
- Conclude: Q

Godel's Incompleteness Theorem

- All Axioms for the Natural Numbers are either Inconsistent or Incomplete.
- There are Formulas in Arithmetic that are True, but that cannot be Proved.

<u>Disjunctive Normal Form</u>

Construction

- For each row in the truth table where $F(p, q, r, \ldots)$ has the value True
    - For each column with a primitive proposition p
        -- Write *p* if *p* has the value *T*
        -- Write *~p* if *p* has the value *F*
- Let $F^*(p, q, r, \ldots) = p \wedge q \wedge \sim r \cdots$ {AND the columns}

  -- Then $F^*(p, q, r, \ldots)$ has the value *T* only along this row
- Let $F(p, q, r, \ldots) = F_1(p, q, r, \ldots) \vee F_2(p, q, r, \ldots) \vee \cdots \vee F_n(p, q, r, \ldots)$

Remarks

- <u>AND</u> has only one row with *T*
- <u>OR</u> has value *T* whenever one of its parameters has value *T*

Examples

- $p \oplus q \equiv (p \wedge \sim q) \vee (\sim p \wedge q)$

Functionally Complete

Definition

A collection of operators are called *functionally complete* if every proposition is equivalent to a proposition involving only these operators.

Proposition 1: The operators ~, ∧, ∨ are functionally complete.

Proof: Follows from Disjunctive Normal Form.

Proposition 2: *The operators ~, ∧ are functionally complete.*

Proof: Follows from Proposition 1 and De Morgan's Laws.

Proposition 3: The operators ~, ∨ are functionally complete.

Proof: Follows from Proposition 1 and De Morgan's Laws.

Functionally Complete (continued)

Proposition 4: The operator NAND is functionally complete.

Proof: Homework

Proposition 5: The operators NOR is functionally complete.

Proof Homework.

Remark

- Propositions 4 and 5 are important in the design of logical gates.

SAT

Definition

- A compound statement is said to be ***satisfiable*** if there is an assignment of truth values to the variables in the statement that makes the statement True.

P vs. NP

- Determining in general whether a compound statement is satisfiable is an NP problem.
- Can be verified in polynomial time, but no solution yet in polynomial time.
- Only exponential time algorithms exist -- try all possibilities.

Part II:

Predicate Calculus

Predicates

Definition

- A Statement with Parameters,
- A Formula

Examples

- $P(x), Q(x,y)$
- $x > 0$, $x + y = z$

Predicate Calculus

- Study of Predicates and Quantifiers

<u>Quantifiers</u>

All

-- $\forall x P(x)$ <u>means</u> for all x, $P(x)$ is True

-- $\forall x P(x)$ is false when there is an x for which $P(x)$ is False

-- analogous to infinite AND

Exists

-- $\exists x P(x)$ <u>means</u> there exists at least one x for which $P(x)$) is True

-- $\exists x P(x)$ is false when $P(x)$ is False for every x

-- analogous to infinite OR

Domain

-- Usually there is some <u>universal set</u> or <u>domain</u> implicitly understood.

-- To be more explicit, we can write $\forall x \in Q \;\; P(x)$.

Syllogism

All men are mortal.	$\forall x P(x) \rightarrow M(x)$	
Socrates is a man.	$P(s)$	{s=constant)
Therefore Socrates is mortal.	$M(s)$	

<u>Dummy Variables</u>

Definition

- x is a dummy variable means that x can be replaced by y.

Examples

- $\forall x P(x)$
- $\int f(x)\, dx$
- *(lambda(x) (+x x))*

Bound and Free

Examples

- $\forall x(\ldots P(x)\ldots)$ -- x is bound to $\forall x$

- $\forall x(x < y)$ -- x is bound, y is free

- Free and bound apply only with respect to a specific scope

  -- $\forall x\left\{\left(\exists x P(x)\right)\vee\left(\forall y(y > x)\right)\right\}$

  -- different x's

  -- different scopes

Scope

Rules

1. A name (variable) refers to the innermost definition for that name.
2. Misuse of scope = common pitfall
3. Variables with no quantifiers, depend on context!
   a. $\sin^2 x + \cos^2 x = 1$ -- $\forall x$
   b. $x^3 - 2x + 1 = 0$ -- $\exists x$
4. Official Rule
   a. free variables are implicitly quantified by $\forall$
5. Practical Rule
   a. depends on context
   b. get clarification

Substitution

Definition

- $P(t|x)$ means result of substituting t for x

  -- t = term, x = variable

Example

- $P(x) = \exists y(y > x)$

  -- $P(t|x) = \exists y(y > t)$

  -- $P(3z^2 + 2|x) = \exists y(y > 3z^2 + 2)$

Capture

$P(x) = \exists y(y > x)$

$P(y|x) = \exists y(y > y)$ -- illegal, common pitfall

Rules for Manipulating Predicates

1. $\forall x \forall y P(x,y) = \forall y \forall x P(x,y)$
2. $\exists x \exists y P(x,y) = \exists y \exists x P(x,y)$

3. $\exists x \forall y P(x,y) \rightarrow \forall y \exists x P(x,y)$
    - $\exists x \forall y P(x,y)$ -- *x* cannot depend on *y*
    - $\forall y \exists x P(x,y)$ -- *x* can depend on *y* {*x(y)*}

4. $\sim \forall x P(x) = \exists x \sim P(x)$ De Morgan's
5. $\sim \exists x P(x) = \forall x \sim P(x)$ Laws

6. $\forall x\{P(x) \wedge Q(x)\} = \{\forall x P(x)\} \wedge \{\forall x Q(x)\}$ Associativity and
7. $\exists x\{P(x) \vee Q(x)\} = \{\exists x P(x)\} \vee \{\exists x\, Q(x)\}$ Commutativity Laws

Rules for Manipulating Predicates (continued)

8. $\forall x\{P(x) \vee Q(x)\} \leftarrow \{\forall x P(x)\} \vee \{\forall x Q(x)\}$ And/Or
    - $\{\forall x P(x)\} \vee \{\forall x Q(x)\}$ -- different *x* for *P* and *Q*
    - $\forall x\{P(x) \vee Q(x)\}$ -- same *x* for *P* and *Q*

9. $\exists x\{P(x) \wedge Q(x)\} \rightarrow \{\exists x P(x)\} \wedge \{\exists x\ Q(x)\}$ Don’t Commute
    - $\exists x\{P(x) \wedge Q(x)\}$ -- same *x* for *P* and *Q*
    - $\{\exists x P(x)\} \wedge \{\exists x\ Q(x)\}$ -- different *x* for *P* and *Q*

10. If *x* is not free in *P*, then
    - $P = \forall x P(x)$
    - $P = \exists x P(x)$

11. $\forall x\{P(x) \leftrightarrow Q(x)\} = \forall x\{P(x) \rightarrow Q(x)\} \wedge \forall x\{Q(x) \rightarrow P(x)\}$

Analogies

1. $\forall \cong$ AND

2. $\exists \cong$ OR

Note these analogies are exact over finite domains.