DM

11 September 2023 07:10 PM

Proposition

→ a statement with value true or false.

Conditional Statements

$p \to q$ if p then q (implificator operator)

i) q is necessary for p

ii) q follows from p

iii) p only if q

iv) q whenever p

v) p is sufficient for q

Properties

$p \to q \equiv \sim q \to \sim p \equiv \sim p \vee q$

Contrapositive

Converse $q \to p$

inverse $\sim p \to \sim q$

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

Laws

Idenpotent $p \vee p \equiv p$

$p \wedge p \equiv p$

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

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

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

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

De Morgan's $\sim(p \vee q) \equiv \sim p \wedge \sim q$

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

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

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

Formulas

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

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

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

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

CNF (Conjunctive Normal form)

if a statement is represented as conjunction of clauses.

DNF (Disjunctive Normal Form)

If a statement is represented as disjunction of statements.

Logical Implification

$p \to p \vee q$ addition

$p \wedge q \to p$ simplification

$[p \wedge (p \to q)] \to q$ Modus Ponens

$[(p \to q) \wedge \sim q] \to \sim p$ Modus Tollens

$[\sim p \wedge (p \vee q)] \to q$ Disjunctive Syllogism

$[p \to q \wedge q \to r] \to (p \to r)$ Hypothetical Syllogism

$$[(p \to q) \wedge (r \to s)] \to [(p \wedge r) \to (q \wedge s)]$$
$$[(p \leftrightarrow q) \wedge (q \leftrightarrow r)] \to [p \leftrightarrow r]$$

Methods

→ first assign propositions to all the statements. (like p, q)

→ then form all the propositional statements (like $p \vee q$)

→ then apply the logical implifications to reach at conclusion.

$(p \to q) \wedge q \to p$ fallacy of affirming the conclusion.

$(p \to q) \wedge \sim p \to \sim q$ fallacy of denying the hypothesis.

Resolution Principle.

$C_1 \equiv C_1' \vee L \qquad C_2 = C_2' \vee \sim L$

if $C_1 \wedge C_2 \equiv$ true then $(C_1' \vee C_2') \equiv$ true also

↳ resolvent of C_1 C_2

$C_1 \wedge C_2 \to C_1' \vee C_2'$ tautology.

Method

→ Build a resolvent tree

→ compute the resolvent and add it to the tree

→ Stop when no more resolerement is possible.

→ the final CNF is our resolution.

Properties

1) $S = \{ C_1 \; C_2 \; C_3 \; - - - \; C_n \}$

if False $\in$ resolvent (S)

then $C_1 \wedge C_2 \wedge \dots C_n \equiv$ False

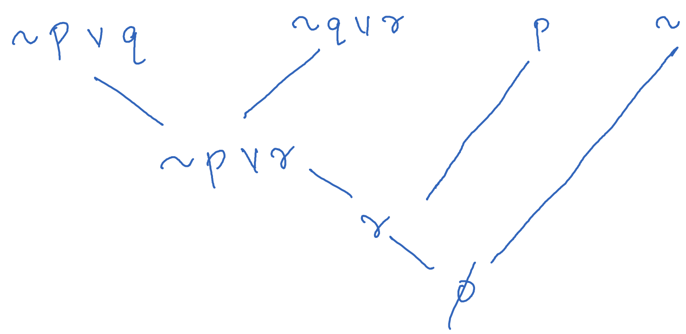
Proof by Resolution

Proof by Resolution

$S = \{ c_1, c_2 \text{ ---- } c_n \}$ $\quad C_i$ = clause

$c \in$ resolvent (S) iff $S \cup \{\sim c\}$ is unsatisfiable.

example
$p1 : \; p \to q \equiv \sim p \vee q$
$p2 : \; q \to r \equiv \sim q \vee r$
$p3 : \; p \to r \equiv \sim p \vee r$
$\sim p3 : \; \sim(p \to r) \equiv \sim r \wedge p$



Predicates.

generalisation / representation of statements. $P(x)$

universe of discourse / domain → set of values of x for which $P(x)$ is defined.

A predicate becomes a proposition when it is assigned a value.

Quantifiers:

1) Universal Quantifier $\forall x \, P(x)$

$\forall x \, P(x) \equiv P(x_1) \wedge P(x_2) \cdots \wedge P(x_n)$ $\quad$ Domain $= \{x_1, x_2 \text{ ---- } x_n\}$

2) Existential Quantifier

$\exists x \, P(x) \equiv P(x_1) \vee P(x_2) \vee \cdots P(x_n)$ $\quad$ Domain $= \{x_1, x_2 \ldots x_n\}$

3) Uniqueness Quantifier.

$\exists! \, x \, P(x) \leftrightarrow \exists x \left[P(x) \wedge y : (P(y) \to y = x) \right]$

$$\exists!\, x\, P(x) \iff \exists x \left[P(x) \wedge y : \left(P(y) \rightarrow y = x \right) \right]$$

Imp Points

1) Every student $\quad \forall x \left[S(x) \rightarrow P(x) \right]$
2) Some students $\quad \exists x \left[S(x) \wedge P(x) \right]$

De Morgans Law

1) $\sim \left[\forall x : P(x) \right] \equiv \exists x : \sim P(x)$
2) $\sim \left[\exists x : P(x) \right] \equiv \forall x : \sim P(x)$

Rules Of Inference

1) Universal Instantiation

$\forall x\, P(x) \Rightarrow P(c)$ is true for any arbitary element c in the universe of discourse

2) Universal Generalisation

$P(c)$ is true for any arbitary element c in domain $\Rightarrow \forall x\, P(x)$

3) Existential Generalisation

$\exists x\, P(x) \Rightarrow P(c)$ is true for some arbitary element c in U

4) Existential Instantiation

$P(c)$ is true for some c in $U \Rightarrow \exists x\, P(x)$

Method

→ First define domain U

→ assign predicates to statements

→ make CNFs of statements

→ Apply rules of inference to convert to propositions.
→ Apply rules of inference for propositions to reach to conclusion.

Methods of Proving

1) Direct Proof

$$[p \wedge (p \rightarrow q)] \rightarrow q$$

Show that conclusion is true assuming principle hypothesis is true.

2) Indirect Proof

A) Proof by Contrapositivity

$$p \rightarrow q \equiv \sim q \rightarrow \sim p$$

use when direct proving technique is not working

B) Vacous Proof

$p \rightarrow q$ if p is a false statement irrespective of q.

c) Proof by Contradiction

if prove $p \rightarrow q$

show $[(p \wedge \sim q) \rightarrow F]$ is tautology

assume $\sim q$ to be true.

Proof By Contradiction

→ to show that p is true by contradiction.
→ assume that a Statement r is true. and $\sim p$ is true.
→ using p and r arrive at $\sim r$ is true.
→ $[\sim p \rightarrow (r \wedge \sim r)]$ ie $[\sim p \rightarrow F]$

$\rightarrow \left[\sim p \rightarrow (r \wedge \sim r) \right]$ ie $\left[\sim p \rightarrow F \right]$

$\Rightarrow \Leftarrow$

Proof Strategies:

i) $(P_1 \wedge P_2 \wedge \dots P_n) \rightarrow Q$ proof by example.

ie $(\sim Q \rightarrow \sim P_1) \vee (\sim Q \rightarrow \sim P_2) \dots \vee (\sim Q \rightarrow \sim P_n)$ is true.

2) $(P_1 \vee P_2 \vee \dots P_n) \rightarrow Q$ proof by cases

ie $(P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q) \dots \wedge (P_n \rightarrow Q)$ is true

We can use Without Loss Of Generalisation (WLOG) when our cases are not given a specific value but are variable.

Non Constructive Proof.

generate such a case, such that without knowing the true value of the case we can arrive at a conclusion

like $(\sqrt{2})^{\sqrt{2}} \rightarrow$ irrational then $\left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}}$ is rational

$\rightarrow$ rational.

Uniqueness Proof.

P1: there exists a sample x that satisfies the property

P2: there exists no other sample other than x which satisfies the property.

Backwards Reasoning

→ To prove that q is true.

→ device a statement p such that $p \rightarrow q$ is true.

* basically reverse engineering

Proof by Mathematical Induction.

1) Regular Induction

to prove $\forall n\ P(n)$

base case: $P(b)$ is true for a specific b

inductive hypothesis: $P(k)$ is true for some $b \geq k$

inductive step: $P(k+1)$ is true from $P(k)$

$$
\begin{array}{l}
\therefore\ P(k) \to P(k+1) \quad \forall\ k \geq b \\
\therefore\ P(b) \\
\hline
\therefore\ \forall n\ P(n) \quad n \geq b.
\end{array}
$$

b) Strong Induction

base case: $P(b)$ true for a specific b

inductive hypothesis: $P(b) \wedge P(b+1) \dots P(k)$ is true for some $b \geq k$

inductive step: $P(k+1)$ is true.

$$
\begin{array}{l}
\therefore\ P(b) \\
\forall k\ P(b) \wedge P(b+1) \dots P(k) \\
\hline
\forall n\ P(n)
\end{array}
$$

Fundamental theorem of Algebra:

$\forall n \in \mathbb{Z}^{+} \quad n = 2^a 3^b 5^c \dots$

any positive integer n can be represented as product of powers of prime no.

SETS

1) Equality of sets $A = B$

iff $A \subseteq B$ and $B \subseteq A$

or $\forall x \ (x \in A \leftrightarrow x \in B)$ is tautology

2) Cardinallity of set = number of elements in set A $n(A) = |A|$

3) Power set $S(A)$
set of all subsets of A $|S(A)| = 2^{|A|}$

4) Subset of A $A \subseteq B$
$\forall x \ (x \in A \rightarrow x \in B)$

cartesian product $A \times B = \{ (a,b) : (a \in A) \wedge (b \in B) \}$

Difference of Sets

$A - B = \{ x : x \in A \wedge x \notin B \}$

Symmetric Difference of Sets.

$A \Delta B = (A - B) \cup (B - A)$

RELATIONS

relation R defined on set A & B

$R \subseteq A \times B$ $|A| = n$ $|B| = m$ $|R| \leq n * m$

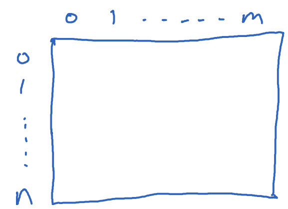
R is defined on set A & B if $a \in A$ and $b \in B$ and $(a,b) \in R$
representation aRb

Matrix Representation

$|A| = m \quad |B| = n \quad$ matrix $M = m \times n$

relation R defined on set A & B $\quad R \subseteq A \times B$

if $(a_i, b_j) \in R$ then $M_{i,j} = 1$ else $M_{i,j} = 0$

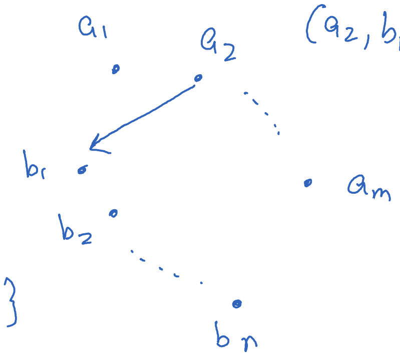


Binary Relations / Graph Relations.

$A = \{a_1\ a_2\ \cdots\ a_m\}$ $\quad B = \{b_1, b_2\ \ldots\ b_n\}$

if $(a_i, b_j) \in R$ connect vertex a_i & b_j

Vertex $V = \{a_1\ a_2 \cdots a_m, b_1, b_2 \cdots b_n\}$



$(a_2, b_1) \in R$

Types of Relations

1) Reflexive relations

relation R defined from set A to itself

$\forall a \in A \left[(a,a) \in R \right]$ is true

diagonal elements $= 1$ in matrix

graphs should have self loops.

$\forall a \left[a \in A \rightarrow (a,a) \in R \right]$

ϕ is a reflexive relation.

if $|A| = n$ then $2^{n^2 - n}$ reflexive relations possible.

2) Irreflexive Relation

$\forall a \left(a \in A \rightarrow (a,a) \notin R \right)$

ϕ is a irreflexive relation.

3) Symmetric Relation.

3) Symmetric Relation.

R is defined from set A to set B

$\forall a \in A, \forall b \in B \left[(a,b) \in R \rightarrow (b,a) \in R \right]$

Matrix must be symmetric
graph should have loops.

4) Asymmetric Relation.

$R \subseteq A \times B$

$\forall a \in A, \forall b \in B : \{ (a,b) \in R \rightarrow (b,a) \notin R \}$

diagonal elements $= 0$ & no $M_{i,j} = M_{j,i}$

5) Anti Symmetric Relation.

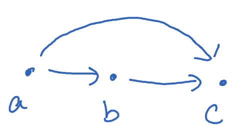
$\forall a \in A, \forall b \in B : \{ (a,b) \in R \wedge (b,a) \in R \rightarrow b = a \}$

if $a \neq b$ then :	$(a,b) \in R$	$(b,a) \in R$
	1	0
	0	1
	0	0

* $\emptyset$ can satisfy reflexive, symmetric, asymmetric, antisymmetric relations.

6) Transitive Relations.

if $a,b,c \in A \{ (a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R \}$



graph

Operations on Relations.

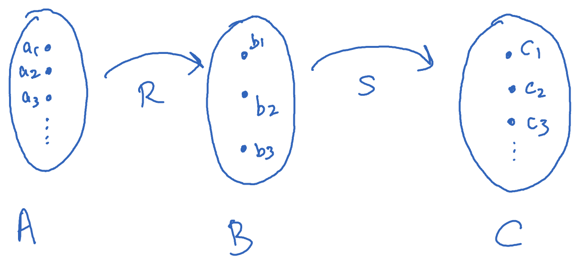
1) intersection $\cap$
2) union $\cup$

2) union $\cup$

3) Difference $-$

4) XOR $\oplus$ $\quad A \oplus B = (A-B) \cup (B-A)$

SoR relations



$R \subseteq A \times B$

$S \subseteq B \times C$

$R^m = R^{m-1} \circ R$

$$S \circ R = \{ (a_i, c_k) : \exists\, b_j \in B \wedge (a_i, b_j) \in R \wedge (b_j, c_k) \in S \}$$

$\forall m \ (a_i, a_j) \in R^m$ interpretation: there exists a path of length m from a_i to a_j in the graph

$$a_i \to a' \to a'' \to a''' \to a_j$$

Closure of a Relation.

1) Reflexive closure: MINIMAL superset such that all (a_i, a_i) are present in that relation.

Reflexive closure of $R = R \cup \{ (a_1, a_1), (a_2, a_2) \dots, (a_n, a_n) \}$

2) Symmetric Closure: MINIMAL superset

$$R \cup \underbrace{\{ (b_j, a_i) : (a_i, a_j) \in R \}}_{R^{-1}}$$

$\therefore R \cup R^{-1} =$ symmetric closure.

3) Transitive closure: MINIMAL superset. is made using recursion.

Properties.

1) a relation R is transitive iff $R^n \subseteq R$

$\Rightarrow$ $R^n \subseteq R$

$(a,b) \in R$ $(b,c) \in R$ $R^2 = R \circ R$ $\therefore$ $(a,c) \in R^2$

But $R^2 \subseteq R$ $\therefore$ $(a,c) \in R$

$\therefore$ $(a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R$

$\Leftarrow$ R is transitive

Base case: $n = 1$ true

Hypo: $R^n \subseteq R$ for all $1 \le i \le n$

step: $R^{n+1} \subseteq R$

suppose $(a,c) \in R^{n+1}$ $\therefore$ $\exists x$ st $(a,x) \in R^n$ $(x,c) \in R$

$R^n \subseteq R$ $\therefore$ $(a,x) \in R \wedge (x,c) \in R$

$(a,x) \in R \wedge (x,c) \in R \longrightarrow (a,c) \in R$

TRANSITIVE CLOSURE

Connectivity relation $R^* = R \cup R^2 \cup R^3 \ldots . R^{|R|}$

$(a_i, a_j) \in R^*$ iff there exists a path of any length b/w a_i & a_j

R^* is the transitive closure of R.

$S \circ R = M_R \odot M_S$ M_R = relation matrix of $R \subseteq A \times B$

boolean product M_S = relation matrix of $S \subseteq B \times C$

Let R be a relation. R^* be its connectivity set.

Let S be a transitive set containing R^*

R^* = transitive relation

S = transitive set then $S^n \subseteq S$

$S^* = S \cup S^2 \cup S^3 \ldots S^n$ $\quad S^* \subseteq S$

if S is transitive then $R \subseteq S$, $R^* \subseteq S$

if $(a,b) \in R^n \Rightarrow (a,b) \in S$

as $R \subseteq S$ $\quad R^n \subseteq S^n$ $\quad R^* \subseteq S^*$

Now if $(a,b) \in R^*$ then $(a,b) \in S^*$

since $S^* \subseteq S$ $\quad (a,b) \in S$

$\therefore$ if $(a,b) \in R^*$ then $(a,b) \in S$

$\therefore$ for any transitive relation S whose subset is R, R^* is also a subset for S

$\therefore$ R^* is smallest transitive relation.

Algorithm's to Calculate Connectivity Closure

1) Naive Algorithm

R = relation on a set $A = \{a_1\ a_2 \ldots a_n\}$

$M_R = n \times n$ matrix

$M_{R^*} = n \times n$ matrix with $M_{ij} = 1$ iff $\exists$ path from a_i to a_j

$M_{R^i} = M_R \odot M_{R^{i-1}}$

$M_{R^*}[i,j] = M_R[i,j] \vee M_{R^2}[i,j] \vee M_{R^3}[i,j] \ldots\ldots$

Time Complexity $O(n^4)$

2) Warshall's Algorithm

Define a sequence of matrices $W_0\ W_1 \ldots W_n$

$W_0 = M_R$

$W_K[i,j] = 0$ if there exists a direct path from i to j with all intermediate nodes from $\{1, 2, \ldots K\}$

→ No restriction in path length.

→ No need for all nodes from $\{1, 2 \ldots K\}$ to be present at the same time.

$W_n = M_{R^*}$

Time complexity $O(n^3)$

EQUIVALENCE RELATIONS

a relation R defined over a set A is equivalent iff:

1) R is reflexive $\forall a \in A\,((a,a) \in R)$ is true.
2) R is symmetric $\forall a,b \in A\,((a,b) \in A \rightarrow (b,a) \in A)$
3) R is transitive $\forall a,b,c \in A\,((a,b) \in A \wedge (b,c) \in A \rightarrow (a,c) \in A)$

$a \equiv b \pmod{m}$ Relation.

if $a \% m = b \% m$ $m \in \mathbb{Z}$

$a \equiv b \pmod{m}$ is reflexive, symmetric & transitive.

EQUIVALENCE CLASSES

If R is a equivalence relation defined on set A and $a \in A$ then the equivalence class $[a]$ is the set of all elements in A which are related to each other in relation R.

$[a] = \{b : (a,b) \in R\}$

→ $[a]$ is not empty for every $a \in R$.

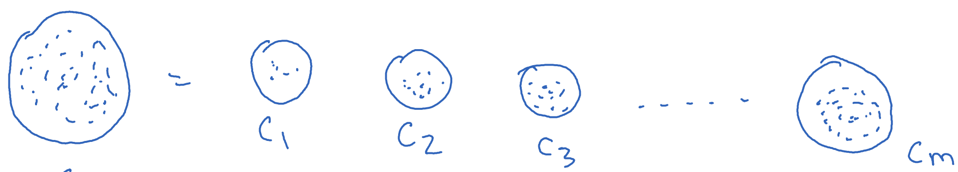
→ $[a]$ is not empty for every $a \in R$.

→ two equivalent classes are either same or disjoint.

Theorem $(a,b) \in R \longleftrightarrow [a] = [b]$

Partition of a Set.

→ Collection of pairwise disjoint non-empty subsets of C whose union gives C



$C = \{1, 2 \dots n\}$

$$\forall\, i,j \in \{1, 2 \dots m\} \quad i \neq j \quad C_i \cap C_j = \phi$$

$$|C_i| \geq 1 \quad \& \quad |C_j| \geq 1$$

From Equivalence Relation to Partition of a set.

Theorem Let R be an equivalence relation R defined over set C and $[c_1]$, $[c_2] \dots [c_m]$ be the equivalence classes Then $[c_1]\ [c_2] \dots [c_m]$ constitute the partition of set C.

From Partition of a Set to Equivalence Classes.

Let C be a partition set with partitions $C_1\ C_2 \dots C_m$ then there exists an equivalence relation R defined over set C with $C_1\ C_2 \dots C_m$ as the equivalence classes.

of Equivalence classes on set C = # Partions on a set C

$a | b$ means a divides b ie $b = ka \quad k \in \mathbb{Z}$

path length = number of edges in a binary tree.

$$R^{n+1} = R^n \circ R$$

$$M_{R_1} \cup M_{R_2} = M_{R_1} \vee M_{R_2}$$

$$M_{R_2} \cap M_{R_2} = M_{R_1} \wedge M_{R_2}$$

$M_{S \circ R} = M_R \odot M_S$ multiplication of matrix.

$$M_{R^n} = M_{R^{n-1}} \odot M_R$$

Naive Algorithm $O(n^4)$

$A := M_R$

$B = A$

for $i = 2$ to n

$\quad A := A \odot M_R$

$\quad B = B \vee A$

computing $(n-1)$ boolean products

$n^2(2n-1)$ for calculating boolean product

$\therefore\ n^2(2n-1)(n-1) = O(n^4)$

Warshall's Algorithm $O(n^4)$

$W := M_R$

for $k = 1$ to n

$\quad$ for $i = 1$ to n

$\quad\quad$ for $j = 1$ to n

$\quad\quad\quad W[i,j] = W[i,j] \vee \left(W[i,k] \wedge W[k,j] \right)$

the returned W will be R^*

Q) find the matrix relation for $P(\{a,b,c\})$

$R: \{ (x,y) : x \subseteq y \}$

For the answer, the graph is created by the vertices being the subsets of $\{a, b, c\}$ and two subsets being directly connected if the former is a subset of the latter. Therefore, we take our vertex set in the order : $\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. So the row for $\{a\}$ will look like $[0, 1, 0, 0, 1, 1, 0, 1]$ because that is the subsets which contain a according to our order. Therefore , creating the matrix gives :

$$\begin{array}{cc}
 & \begin{array}{cccccccc} \emptyset & a & b & c & a,b & b,c & c,a & a,b,c \end{array} \\
\begin{array}{c} \emptyset \\ \{a\} \\ \{b\} \\ \{c\} \\ \{a,b\} \\ \{b,c\} \\ \{a,c\} \\ \{a,b,c\} \end{array} &
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\end{array}$$

* be careful of the domain & always list it

$R = \{ (a,b) : a \text{ divides } b \}$

Domain = $\mathbb{R}$ then R is not reflexive (0,0) problem

Domain = $\mathbb{Z}^+$ then R is reflexive.